

Toekomstverkenning klimaatrisico's voor de digitale infrastructuur

TNO 2026 R10005 – 30-03-2026

Toekomstverkenning klimaatrisico's voor de digitale infrastructuur

Auteurs	Marcel van Sambeek, Corine Bonte, Paula Broekman, Marth Breure, Jip van Stijn, Pieter Verstraten
Rubricering rapport	TNO Publiek
Titel	TNO Publiek
Rapporttekst	TNO Publiek
Aantal pagina's	122 (excl. voor- en achterblad)
Aantal bijlagen	0
Opdrachtgever	Planbureau voor de Leefomgeving (PBL)
Programmanaam	Klimaatrisicoanalyse 2022-2026
Programmanummer	PBL
Projectnaam	PBL Herijking klimaatrisico's 2024-2025
Projectnummer	060.59480

Alle rechten voorbehouden

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van TNO.

© 2026 TNO

Samenvatting

Aanleiding

In 2014/2015 is de eerste nationale klimaatrisicoanalyse uitgevoerd door het Planbureau van de Leefomgeving (PBL) ter ondersteuning van de nationale klimaatadaptatiestrategie (NAS) in 2016. In 2021 is besloten om opnieuw een klimaatrisicoanalyse te laten uitvoeren voor een herziening van de NAS. Er zijn meerdere redenen voor herziening. Klimaatgebeurtenissen doen zich vaker en heftiger voor dan verwacht. Dit leidt tot een toenemend bewustzijn van de noodzaak tot adaptatie bij beleid, politiek en algemeen publiek. Ook leiden recent ervaren klimaatgebeurtenissen zoals overstromingen, wateroverlast, droogte, hitte en stormen tot nieuwe kennis en data over het verband tussen klimaatgebeurtenis en impact.

Het PBL is gevraagd om de hernieuwde klimaatrisicoanalyse uit te voeren in de periode 2022–2026. In deze analyse brengen de kennisinstituten de klimaatrisico's voor klimaatgevoelige vitale sectoren en beleidsterreinen in kaart, door PBL samengevoegd in een overkoepeld rapport. TNO heeft de analyse uitgevoerd voor de sectoren Gebouwde Omgeving en ICT. In dit rapport zijn de resultaten beschreven van de klimaatrisicoanalyse voor de sector ICT. Het betreft de klimaatrisico's voor de fysieke elementen in de digitale infrastructuur in Nederland, zoals glasvezelkabels, masten en andere opstelpunten, technische gebouwen voor mobiele en vaste netwerken en datacenters.

Onderzoeksmethodiek PBL

Voor de toekomstverkenning is de systematiek opgesteld door het PBL. Deze is gebruikt door alle kennisinstituten voor de klimaatrisicoanalyse. Voor de analyse naar toekomstige klimaatrisico's zijn zogeheten contextscenario's en adaptatiescenario's gebruikt om toekomstige ontwikkelingen en mogelijke maatregelen, binnen een verwachte bandbreedte, te beschrijven.

De twee contextscenario's omvatten toekomstige ontwikkelingen op het gebied van klimaatverandering én maatschappelijke ontwikkelingen voor de zichtjaren 2050 en 2100. Klimaatverandering en maatschappelijke ontwikkelingen zijn gecombineerd tot één beperkt risicoverhogend scenario en één sterk risicoverhogend scenario. Voor de klimatologische ontwikkelingen zijn twee van de vier scenario's van de KNMI'23 klimaatscenario's voor Nederland gekozen: het contextscenario 'Beperkt risicoverhogend' op basis van het KNMI 'Ln scenario' (Lage uitstoot / beperkte klimaatverandering, natte omstandigheid), en het contextscenario 'Sterk risicoverhogend' op basis van KNMI'23 'Hd' scenario (Hoge uitstoot / grote klimaatverandering, droge omstandigheden). Daarmee gebruiken we de grootste bandbreedte voor alle KNMI'23 klimaatrisico's die te maken hebben met droogte en watertekort. Voor de maatschappelijke ontwikkelingen zijn demografische, socio-economische en technologische ontwikkelingen meegenomen in de twee contextscenario's. Voor ICT is een (zeer) sterke toename van digitalisering en de bijbehorende vraag naar ICT voorzien, en een (zeer) sterke toename van de verwevenheid van de sector ICT met andere sectoren.

Voor de klimaatrisicoanalyse is gebruik gemaakt van drie adaptatiescenario's:

1. Huidige beleid: Het eerste adaptatiescenario omvat het huidige beleid en -maatregelen: In dit scenario wordt het huidige klimaatadaptatiebeleid doorgetrokken naar de toekomst, d.w.z. voor de twee contextscenario's.

Daarnaast zijn er twee aanvullende toekomstige adaptatiescenario's:

2. Transformeren: dit scenario heeft een ruimtelijke focus. We gaan er in dit scenario van uit dat er bij ontwikkelingen in hoge mate rekening wordt gehouden met het water en de bodem. Dit scenario is meer transformatief van aard en draait meer om het verminderen van de blootstelling van mensen en objecten aan klimaatverandering; hier speelt dus locatie een belangrijke rol.
3. Intensiveren: dit scenario heeft een technische focus: dit scenario is gericht op het doorontwikkelen en intensiveren van het huidige beleid en vooral gericht op oplossingen via technische maatregelen, waarbij we in grote lijnen dezelfde dingen blijven doen op dezelfde locaties, maar de effecten van klimaatverandering zoveel mogelijk verkleinen. Daarmee is dit scenario meer incrementeel, reactief van aard, en vooral gericht op het beperken van de gevoeligheid van mensen en objecten voor klimaatverandering.

Digitale infrastructuur in Nederland

De digitale infrastructuur is het geheel aan schakels dat de eindgebruiker in staat stelt om toegang te krijgen tot digitale content en applicaties. De digitale infrastructuur vormt de basis voor het leveren van digitale diensten (internet, cloud, etc.) voor consumenten, zakelijke gebruikers en overheden door marktspelers zoals KPN, Odido en VodafoneZiggo, maar ook door cloudaanbieders zoals Amazon, Google en Microsoft. Door de snelle technologische ontwikkelingen binnen de digitale infrastructuur is het voor de periode 2050 tot 2100 onvoldoende duidelijk hoe de fysieke, digitale infrastructuur zich ontwikkelt, binnen Nederland en binnen Europa en wat het effect is op klimaatrisico's. Voor de analyse is daarom alleen gekeken naar de periode tot 2050, niet tot 2100.

In de klimaatrisicoanalyse is gekeken naar de fysieke elementen binnen op de digitale infrastructuur (masten, datakabels (glasvezel), straatkasten en andere netwerkklocaties en datacenters). Hierbij is gekeken naar die elementen die extra aandacht vragen voor te verwachten directe en indirecte gevolgen bij het optreden van klimaatrisico's en voor aanvullende maatregelen om de weerbaarheid binnen de digitale infrastructuur zelf en het gebruik door sectoren te verhogen. In de analyse is de digitale infrastructuur in Nederland en binnen Europa bekeken, niet voor Caribisch Nederland. Hierbij is onderscheid gemaakt in de digitale infrastructuur voor generieke of openbare digitale diensten (zie hoofdstuk 3), en in sectorspecifieke infrastructuur voor bijv. de energiesector, openbare orde en veiligheid, gezondheidszorg (ziekenhuizen) en transport (zie hoofdstuk 7). Binnen de twee contextscenario's ('beperkt' en 'sterk risicoverhogend') zijn globaal ook de verwachte toekomstige ontwikkelingen (trends) binnen de digitale infrastructuur beschreven tot 2050. Voor de periode 2050-2100 is onvoldoende duidelijk hoe de fysieke, digitale infrastructuur zich ontwikkelt, binnen Nederland en binnen Europa. Daarnaast is in de analyse aanvullend gekeken naar sectorspecifieke digitale infrastructuur voor de sectoren openbare orde en veiligheid, energie (elektriciteit), transport en gezondheidszorg.

Klimaatrisicoanalyse digitale infrastructuur

Voor de klimaatrisicoanalyse is eerst een globale analyse uitgevoerd om de grootste directe en indirecte klimaatrisico's in kaart te brengen. De grootste directe klimaatrisico's zijn

verstoringen door hitte, (lokale) wateroverlast en extreem weer van mobiele masten/opstelpunten, en verstoringen door hitte i.c.m. langdurige droogte en lokale wateroverlast bij datacenters. Hitte in combinatie met langdurige droogte kan leiden tot koelproblemen bij extreme hitte en daarnaast het risico op koelwatertekorten bij restricties op watergebruik in een periode van langdurige droogte. De klimaatrisico's voor datakabels en vaste technische locaties zijn beperkt. Het grootste indirecte klimaatrisico is uitval van de elektriciteitsvoorziening, waardoor ook (grote) delen van de digitale infrastructuur uitvallen en de digitale economie en andere sectoren tot stilstand komen.

Voor het adaptatiescenario 'huidig beleid' is gekeken naar geïmplementeerd beleid en huidige wetgeving t.a.v. klimaatrisico's. Hierbij is gekeken naar verschillende beleidsthema's zoals economische beleid, ruimtelijk beleid, duurzaamheid en beleid ten aanzien van de weerbaarheid van vitale digitale infrastructuur in Nederland. Voor de wetgeving is gekeken naar huidige wetgeving (zoals de Telecommunicatiewet (Wet) en beleid- en wetgeving voor datacenters) en naar wetgeving die op korte termijn verwacht wordt zoals de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke). Voor de twee toekomstige adaptatiescenario's met aanvullend beleid (transformeren en intensiveren) zijn door TNO mogelijke aanvullende beleidsmaatregelen verkend om toekomstige klimaatrisico te beperken.

Beleidsboodschappen: opgaven voor de toekomst

Op basis van de klimaatrisicoanalyse zijn door de TNO beleidsboodschappen voor de 3 adaptatiescenario's beschreven.

Voor het adaptatiescenario 'huidige beleid' zijn op basis van klimaatrisicoanalyse beleidsboodschappen opgesteld die beschrijven in hoeverre het huidige beleid en wetgeving (economische beleid, ruimtelijk beleid, duurzaamheid en weerbaarheid van vitale digitale infrastructuur) voldoende is om de toenemende klimaatrisico's tot 2050 af te dekken, ook gelet op de verwachte adaptatiemogelijkheden van de digitale sector zelf en de overheid tot 2050. Op basis van de analyse is de eindimpact bepaald op 'laag' voor i) mens en cultuur (laag aantal doden of ernstig gewonden, lokale en omkeerbare schade), ii) natuur en milieu (lokale en omkeerbare schade voor natuur en milieu) en iii) economie (< € 100 miljoen economische schade per jaar). Mogelijke uitzonderingen met grotere economische impact zijn een grote regionale of landelijke stroomstoring die meerdere uren duurt, een regionale overstroming waarbij schade ontstaat aan gebouwen en apparatuur in een groter gebied, en keteneffecten bij uitval van individuele datacenters of kritieke ICT-voorzieningen binnen vitale sectoren (anders dan ICT). Deze laatste zijn moeilijk in te schatten door de complexiteit binnen ketens en continue veranderingen binnen ketens van ICT-diensten en –voorzieningen. Keteneffecten kunnen uiteindelijk wel voor grote maatschappelijke ontwrichting zorgen als dit bijv. leidt tot uitval van vitale processen.

Voor de adaptatiescenario's 'transformeren' en 'intensiveren' zijn mogelijke aanvullende beleidsmaatregelen beschreven om de impact van klimaatrisico's op mens en cultuur, natuur en milieu en economie verder te verlagen. De belangrijkste beleidsboodschappen voor het adaptatiescenario 'transformeren' zijn:

- Een hoogwaardige digitale infrastructuur in Nederland en Europa is en blijft belangrijk voor economische groei. Een volledig nationaal verbod op nieuwe hyperscale datacenters vermindert de klimaatrisico's voor Nederland, maar leidt tot verplaatsing van de opgave naar andere EU-landen en kan de Nederlandse positie binnen de Europese digitale

infrastructuur verzwakken. Daarom ligt het meer voor de hand om geografische spreiding van (hyperscale) datacenters binnen Europa af te stemmen en daarnaast via nationaal ruimtelijk beleid binnen Nederland vorm te geven met specifieke aandacht voor toegang tot duurzame energie (kernenergie, waterstof) gezien de sterke groei in elektriciteitsvraag van datacenters en 'AI factories'.

- Daarnaast is een verbetering van de geografische spreiding van datacenters wenselijk om de systeemkwetsbaarheid voor regionale klimaatincidenten te verkleinen, met een tweede nationale cluster naast MRA (nu >70%). De risico's op verstoringen t.g.v. regionale klimaatrisico's in de MRA-regio, zoals regionale uitval van elektriciteitsvoorziening, regionale overstromingen of regionale watertekorten worden hiermee voor Nederland als geheel sterk verminderd. Geografische spreiding is uiteraard ook mogelijk binnen Europa naar andere datacenterclusters in buurlanden

Voor het adaptatiescenario 'intensiveren' zijn de belangrijkste beleidsboodschappen:

- Onderzoek de mogelijkheid op een volledig verbod op laagwaardig drinkwatergebruik voor datacenters en de overstap naar alternatieven (industriële water, regen- of oppervlaktewater). Mogelijk dat hiervoor ook financiële stimulering vanuit de overheid (subsidies en/of hogere tarifiering voor laagwaardig drinkwatergebruik) voor de overstap naar alternatieven wenselijk is, zowel voor de digitale sector als voor andere sectoren die getroffen worden.
- Neem klimaatrisico's expliciet mee in het ruimtelijk beleid en in de uitvoering van de Wet weerbaarheid kritieke entiteiten (Wwke). Hiermee is het mogelijk om sector brede maatregelen voor de digitale infrastructuur (met vitale telecom en cloudaanbieders) te nemen om de verschillende klimaatrisico's tot 2050 te beperken, bijv. bij lokale wateroverlast, regionale droogte/hitte en regionale stroomuitval (t.g.v. klimaatrisico's). Door verdere aanscherping van (Europese) wettelijke restricties voor de gehele sector (door deze op de korte en middellange termijn strikter worden, lijken de klimaatrisico's tot 2050 (en mogelijk zelfs tot 2100) goed te mitigeren.
- Richt een maatstaf en monitoring in, zodat naleving en het effect van maatregelen voor de verschillende klimaatrisico's over de jaren heen gevolgd kan worden.
- Het effect van het beleid is groter naarmate klimaatrisico's groter zijn.

Beleidsboodschappen sectorspecifieke digitale infrastructuur

Zorg, energie, OOV en transport leunen op dezelfde generieke digitale infrastructuur, met daarnaast eigen ICT-infrastructuur. De sterkte van de generieke digitale infrastructuur zit in professionaliteit en redundantie bij de grotere aanbieders; de zwakte van sectorspecifieke infrastructuur treedt op bij versnipperde ICT-systemen en (beheer)organisatie en bij single-tenant faciliteiten met beperkte (oefening met) uitwijkvoorzieningen. Migratie naar colocatie/cloud kan de fysieke kwetsbaarheid reduceren, mits contractueel geborgd (continuïteit en hersteltijden bij calamiteiten, meerdere cloud zones, fysieke locaties niet in hetzelfde overstromingsbekken).

De grootste maatschappelijke effecten ontstaan wanneer verstoringen elkaar in de keten versterken. In de implementatie van de Wwke en Cbw voor zowel vitale aanbieders binnen de digitale infrastructuur als voor vitale aanbieders in sectoren zoals elektriciteit, OOV, zorg en transport ontstaat ruimte om klimaatrelevante risico's, expliciet en toetsbaar op te nemen in risicobeoordelingen. Een compacte set indicatoren, onder meer locatiehoogte ten opzichte van NAP, herkomst van koelwater, resultaten van tests met noodstroom en koeling, en mate van geografische scheiding tussen primaire en uitwijklocaties, maakt voortgang zichtbaar en ondersteunt gerichte bijsturing.

In samenhang bezien leidt deze benadering tot een stapsgewijze daling van het restrisico. Keuzes over ligging en spreiding verminderen de blootstelling van het systeem, technische en organisatorische eisen verkleinen de kwetsbaarheid, en afspraken in de keten verkorten de hersteltijd tijdens zwaardere scenario's.

Inhoudsopgave

Samenvatting	3
Inleiding	9
1.1 Aanleiding.....	9
1.2 Inhoud van de Nederlandse klimaatrisicoanalyse 2022 – 2026	9
1.3 Doelen en onderzoeksvraag.....	10
1.4 Reikwijdte	11
1.5 Leeswijzer	12
2 Onderzoeksmethodiek PBL	13
2.1 Toekomstverkenning klimaatrisico's	14
2.2 Toepassing systematiek sector ICT	24
3 Digitale infrastructuur in Nederland	26
3.1 Opdeling van de digitale infrastructuur	26
3.2 Hoge mate van beschikbaarheid	29
3.3 Trends	30
4 Klimaatrisico's digitale infrastructuur	34
4.1 Klimaatdreigingen.....	34
4.2 Klimaatrisico's digitale infrastructuur.....	34
4.3 Selectie van klimaatrisico's.....	41
5 Klimaatrisicoanalyse digitale infrastructuur bij huidig beleid	45
5.1 Huidige beleid en wetgeving.....	45
5.2 Masten en hitte.....	48
5.3 Masten en extreem weer.....	53
5.4 Datacenters en combinatie van hitte en droogte	55
5.5 Datacenters en overstromingen.....	67
5.6 Klimaatrisicoanalyse voor digitale infrastructuur als geheel.....	78
5.7 Beleidsboodschappen: opgaven voor de toekomst.....	85
6 Klimaatrisicoanalyse digitale infrastructuur bij aanvullend beleid	88
6.1 Adaptatiescenario's bij aanvullend beleid	89
6.2 Klimaatrisicoanalyse bij aanvullend beleid.....	91
6.3 Beleidsboodschappen met beleidsopties voor aanvullend beleid	96
7 Sectorspecifieke infrastructuur	98
7.1 Openbare orde en veiligheid.....	98
7.2 Elektriciteitsvoorziening	102
7.3 Gezondheidszorg	104
7.4 Transport.....	107
8 Reflecties en conclusies	111
Interviewlijst.....	114
Afkortingen	115
Referenties	117

Inleiding

1.1 Aanleiding

In 2014/2015 is de eerste nationale klimaatrisicoanalyse uitgevoerd door het Planbureau van de Leefomgeving (PBL) [1] [2] [3] ter ondersteuning van de nationale klimaatadaptatiestrategie (NAS) in 2016 [4]. In 2021 is onder de vlag van het Directeurenoverleg Nationale klimaatadaptatiestrategie gezamenlijk besloten om opnieuw een klimaatrisicoanalyse te laten uitvoeren. De resultaten leveren kennis voor een herziening van de NAS. Er zijn meerdere redenen voor een herziening van de klimaatrisicoanalyse en NAS. Klimaatgebeurtenissen doen zich vaker en heftiger voor dan verwacht. Dit leidt tot een toenemend bewustzijn van de noodzaak tot adaptatie bij beleid, politiek en algemeen publiek. Ook leiden recent ervaren klimaatgebeurtenissen zoals overstromingen, wateroverlast, droogte, hitte en stormen tot nieuwe kennis en data over het verband tussen klimaatgebeurtenis en impact.

Het PBL is gevraagd om de hernieuwde klimaatrisicoanalyse uit te voeren in de periode 2022 – 2026. In deze analyse brengen de kennisinstituten de klimaatrisico's per (beleids)sector in kaart, door PBL samengevoegd in [5]. TNO heeft de analyse uitgevoerd voor de sectoren Gebouwde Omgeving [6] en ICT. In dit rapport zijn de resultaten beschreven van de analyse voor de sector ICT.

1.2 Inhoud van de Nederlandse klimaatrisicoanalyse 2022 – 2026

Voor de hernieuwde klimaatrisicoanalyse is door het PBL i) een evaluatie uitgevoerd van de eerste klimaatrisicoanalyse in 2014/2015, ii) zijn de beschikbare standaarden en conceptuele raamwerken onderzocht en iii) is een inventarisatie gemaakt van de bestaande initiatieven en uitgevoerde risicoanalyses in zowel Nederland als het buitenland. De hieruit geleerde lessen zijn opgenomen in een analysemethodiek van de tweede Nederlandse nationale klimaatrisicoanalyse (2022 – 2026). De analysemethodiek is door het PBL uitgewerkt in [7] en deze is gebruikt in de analyse door alle kennisinstituten. TNO heeft deze gebruikt voor de sector ICT en de Gebouwde Omgeving.

De herijking van klimaatimpacts en -risico's door het PBL bestaat uit:

- Een analyse van huidige (afgelopen 30 jaar en trends hierbinnen) en toekomstige klimaatrisico's. Deze analyse is gebaseerd op respectievelijk waarnemingen en op klimaatscenario's die ontwikkeld zijn door het KNMI in 2023 (KNMI'23 klimaatscenario's, zoals beschreven in [8]). De analyse is op nationale schaal en, indien relevant, mogelijk, regionaal gedifferentieerd. De analyse is gericht op meerdere (beleids)sectoren, waaronder ICT en gebouwde omgeving. TNO heeft deze analyse voor toekomstige klimaatrisico's voor de sector ICT (en de onderliggende fysieke digitale infrastructuur in Nederland) uitgevoerd en deze analyse is beschreven in hoofdstuk 5 van dit rapport.

- Voor de toekomstverkenning worden klimaatrisico's voor 2050, 2100 en enkele doorzichten naar 2150 in kaart gebracht. Hierbij wordt een gematigd risicoverhogend en een sterk risicoverhogend scenario gehanteerd op het gebied van klimaatverandering en maatschappelijke (sociaaleconomische en ruimtelijke) ontwikkelingen. Beide contextscenario's zijn beleidsarm qua klimaatadaptatie en vormen zo een referentie voor de effecten van mogelijke adaptatiestrategieën. Deze contextscenario's zijn beschreven in paragraaf 2.1.1.
- Het doorvertalen van de resultaten van beide analyses naar eindrisico's voor mens en cultuur, natuur en milieu en economie, zodat risico's onderling vergelijkbaar zijn. Hierin wordt zowel kwalitatieve als kwantitatieve informatie over klimaatimpacts en -risico's meegenomen.
- Handreikingen voor de prioriteitstelling in de aanpak van deze risico's volgens een systematiek met zo veel mogelijk objectieve criteria voor urgentiebepaling. Hierbij wordt rekening gehouden met de omvang van de risico's, de kwetsbaarheid en het belang van de (beleids)sector, adaptatie acties die al lopen of op de rol staan, meekoppelkansen en samenhang met ontwikkelingen in andere beleidsvelden, gevaren voor maladaptatie (adaptatiemaatregel of maatregel in een ander beleidsveld die onbedoeld het klimaatrisico vergroot in plaats van verkleint) en 'lock-ins' (maatregelen of besluiten met een langdurige uitwerking in een beleidsveld, die een klimaatrisico doen vergroten en lastig of duur zijn om ongedaan te maken), en de snelheid waarmee het risico naar verwachting groeit versus de benodigde tijd voor onderzoeken, ontwerpen en implementeren van adaptatiemaatregelen.
- Een verkenning van adaptatieopties voor de urgente risico's. De basis hiervoor is de analyse van huidige en toekomstige klimaatrisico's, en van de blootstelling aan en kwetsbaarheid van (beleids)sectoren voor deze risico's.
- Het formuleren van handreikingen voor de bepaling van de Nationale klimaatadaptatiestrategie (NAS) op basis van bovenstaande analyses. Hierbij komen ook de rollen en verantwoordelijkheden van verschillende betrokken partijen aan de orde.

De kennisinstituten brengen binnen het onderzoeksprogramma de klimaatrisico's per (beleids)sector in kaart. De resultaten van de sector ICT naar de klimaatrisico's voor de digitale infrastructuur zijn beschreven in dit rapport. Het PBL voert een overkoepelende analyse uit met de bevindingen van deze deelstudies om een risicobeeld te schetsen voor Nederland. Adaptatiestrategieën, sectoroverschrijdende (cascade)effecten en extremen neemt het PBL hier ook in mee.

1.3 Doelen en onderzoeksvraag

Hieronder zijn de doelen en de onderzoeksvraag van het overkoepelende onderzoek van het PBL opgenomen zoals beschreven in [7]. De doelen van de Nederlandse nationale klimaatrisicoanalyse 2022–2026 zijn:

1. *Nulmeting*: uitvoeren van een nulmeting als referentie voor het periodiek uitvoeren van klimaatrisicoanalyses, waarmee de veranderingen in de risico's en de vorderingen richting 'Nederland klimaatbestendig en waterrobuust in 2050' (en daarna) worden verkend. Herhaalde klimaatrisicoanalyse en evaluatie van adaptatie en adaptatiecapaciteit helpen om ontwikkelingen te onderkennen en te volgen, en om kennis te genereren over de effectiviteit van maatregelen [9], [10]. Deze 'nulmeting', gebaseerd op bestaande informatie, betreft zowel de huidige situatie (1990 – 2022) als de verwachte situaties in het midden en einde van de 21e eeuw

(2050, 2100 en enkele doorkijken naar 2150) onder de voorziene klimaatveranderingen (KNMI'23 klimaatscenario's voor Nederland [8]), en sociaaleconomische en ruimtelijke ontwikkelingen, met het geïmplementeerde en huidige (geïnstumenteerde en gefinancierde) adaptatiebeleid.

2. *Identificatie van kwetsbaarheden, inschatting van omvang van risico's en bouwstenen voor prioritering van adaptatie*: vele factoren zijn bepalend voor de blootstelling aan, gevoeligheid voor en adaptatiecapaciteit tegen klimaatdreigingen van (beleids)sectoren. Klimaatrisicoanalyse geeft inzicht in deze factoren en dit helpt om prioriteiten te stellen in de aanpak van risico's. Ook de identificatie van kennislacunes is van belang. De resultaten van de klimaatrisicoanalyse kunnen aangeven waar snel actie nodig is (bijvoorbeeld om 'lock-ins' en toekomstige klimaatimpacts te vermijden) en ze kunnen de noodzaak aantonen voor het ontwikkelen van adaptatiecapaciteit bij bepaalde (beleids)sectoren. Deze kennis kan bijdragen aan de herziening van de NAS. Ook kan het bijdragen aan de bewustwording van de gevolgen van klimaatverandering en de noodzaak tot adaptatie.
3. *Identificatie van aangrijpingspunten voor adaptatie aan klimaatverandering*: zowel het proces van klimaatrisicoanalyse als de eindresultaten ervan kunnen helpen om mogelijke adaptatiemaatregelen te identificeren. Deze kennis kan een brug slaan naar beleid en op basis van de bepaling van urgente risico's het adaptatiebeleid ondersteunen door handreikingen te bieden voor verschillende adaptatie-strategieën.

Het eerste doel is door het PBL opgesteld om zo te anticiperen op een langdurige monitoring en structurele risicoanalyse van klimaatadaptatie. Dit betekent dat de nationale klimaatrisicoanalyse 2022 – 2026 extra aandacht heeft aan een transparante systematiek van de analyse, zodat methoden en keuzes herleidbaar en herhaalbaar zijn en de resultaten vergelijkbaar voor volgende klimaatrisicoanalyses.

De nationale klimaatrisicoanalyse 2022 – 2026 brengt in beeld welke klimaatrisico's in Nederland een bedreiging vormen voor mens en cultuur, natuur en milieu en de economie ('*people, planet, profit*'), in zowel de huidige situatie als mogelijke toekomstige situaties. Deze informatie geeft handvatten voor het bevestigen en zo nodig bijstellen van de urgentie en prioriteiten in de Nationale klimaatadaptatiestrategie (NAS).

1.4 Reikwijdte

De NAS geldt Nederland-breed en gaat over alle klimaatgevoelige sectoren en beleidsterreinen. De nationale klimaatrisicoanalyse 2022 – 2026 ondersteunt de herziening van de NAS. De klimaatrisicoanalyse neemt (beleids)sectoren mee waarvoor het betreffende ministerie betaalt en/of (beleids)sectoren die vitaal en kwetsbaar zijn. Voor de sector ICT (telecomsector) is dit het Ministerie van Economische Zaken.

De klimaatrisicoanalyse neemt ook de verbindingen tussen sectoren en beleidsterreinen in beschouwing. De overzeese gebieden worden voorsnog niet meegenomen bij gebrek aan middelen hiervoor.

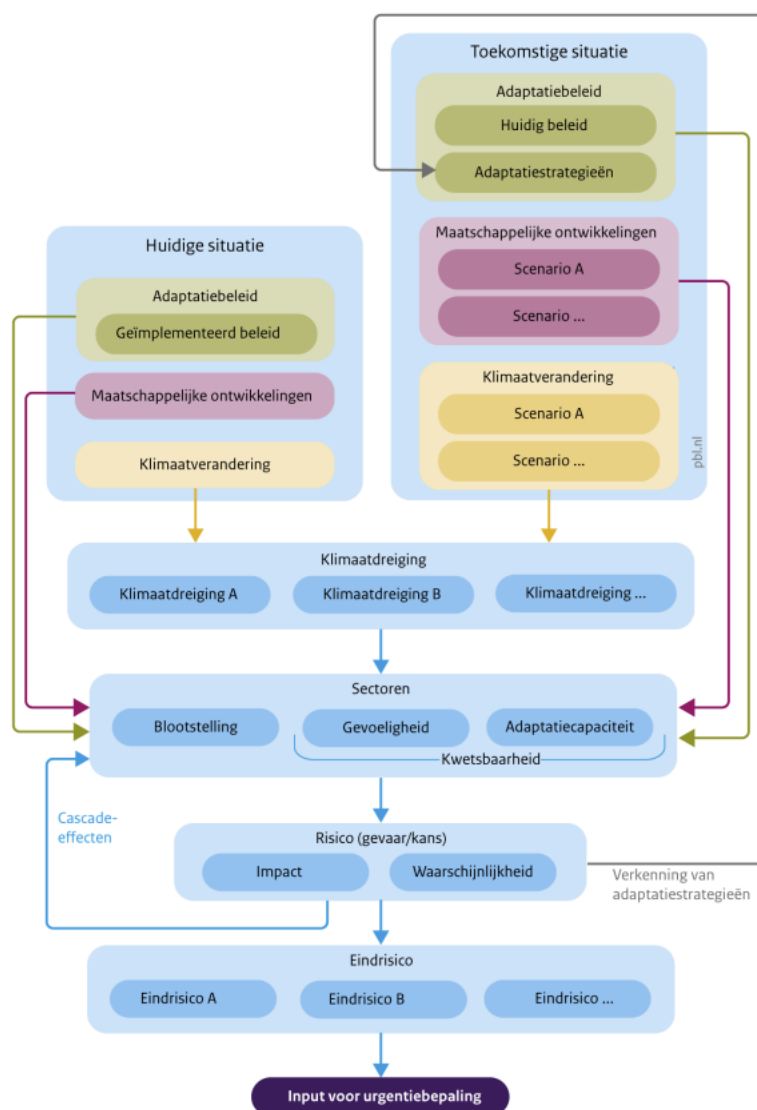
1.5 Leeswijzer

In hoofdstuk 2 is de systematiek beschreven zoals opgesteld door het PBL. Hierbij is ook aangegeven op welke manier TNO deze systematiek heeft toegepast in de klimaatrisicoanalyse voor de sector ICT. In hoofdstuk 3 is de digitale infrastructuur in Nederland beschreven. In hoofdstuk 4 zijn de klimaatrisico's voor de fysieke, digitale infrastructuur (nulmeting), waarbij de belangrijkste of meest relevante klimaatrisico's zijn geïdentificeerd voor nadere analyse bij huidig beleid, zie hoofdstuk 5, en aanvullend toekomstig beleid via twee adaptatiescenario's (transformeren en intensiveren), zie hoofdstuk 6).

In hoofdstuk 7 is aanvullend gekeken naar sectorspecifieke digitale infrastructuur die wordt gebruikt naast de generieke digitale infrastructuur in Nederland, voor de sectoren openbare orde en veiligheid, elektriciteitsvoorziening binnen de sector energie, gezondheidszorg en transport. In hoofdstuk 8 zijn reflecties en conclusies beschreven.

2 Onderzoeksmethodiek PBL

Het conceptueel raamwerk is beschreven in [7], zie Figuur 1. Het raamwerk is aangevuld met meer gedetailleerde uitwerkingen. In dit hoofdstuk is het conceptueel raamwerk beschreven, met een toelichting op de stappen, de definities en de gebruikte scenario's.



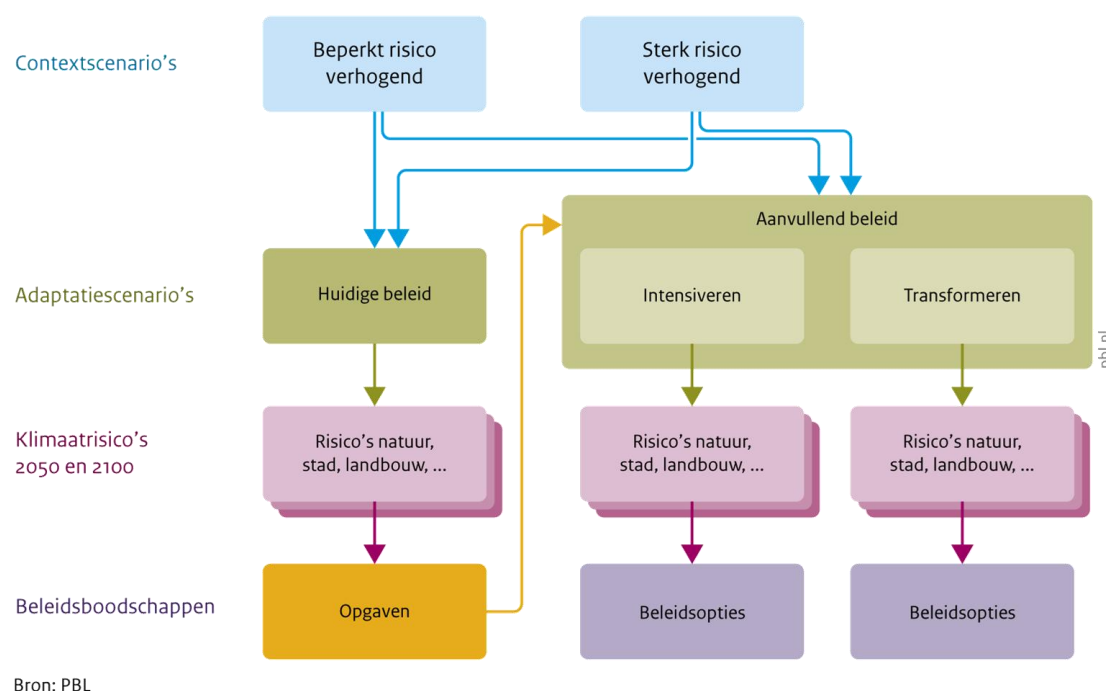
Bron: PBL

Figuur 1 Conceptueel raamwerk Nederlandse klimaatrisicoanalyse (bron: PBL [7])

2.1 Toekomstverkenning klimaatrisico's

Voor de toekomstverkenning is de systematiek zoals opgesteld door het PBL [7] gebruikt, zie Figuur 2.

Verkenning toekomstige klimaatrisico's



Figuur 2 Systematiek voor verkenning toekomstige klimaatrisico's

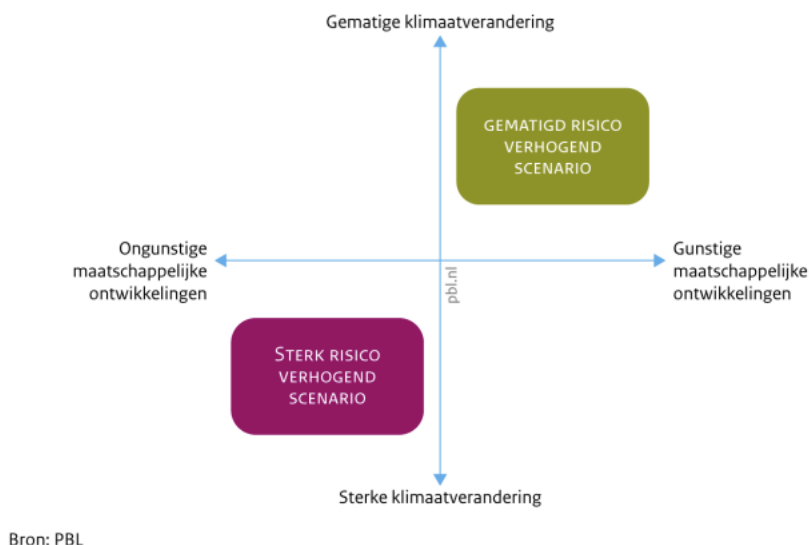
2.1.1 Contextscenario's 'Beperkt risicoverhogend' en 'Sterk risicoverhogend'

Voor de analyse van toekomstige klimaatrisico's worden contextscenario's toegepast, zoals aangegeven in Figuur 2. De contextscenario's omvatten ontwikkelingen op het gebied van klimaatverandering en maatschappelijke ontwikkelingen, zie Figuur 3. Wat betreft klimaatverandering maken we onderscheid tussen gematigde en sterke klimaatverandering. Wat betreft maatschappelijke ontwikkelingen maken we onderscheid tussen gunstige en ongunstige maatschappelijke ontwikkelingen. De termen gunstig en ongunstig zijn bedoeld om aan te geven of maatschappelijke ontwikkelingen een positief dan wel negatief effect hebben op een klimaatrisico. Klimaatverandering en maatschappelijke ontwikkelingen worden gecombineerd tot één gematigd risicoverhogend scenario en één sterk risicoverhogend scenario.

De contextscenario's beschrijven een palet aan ontwikkelingen die van invloed zijn op de toekomstige klimaatrisico's in binnen- en buitenland, en die we als gegeven beschouwen omdat adaptatiebeleid er geen (of beperkt) invloed op heeft. Vanuit het perspectief van onze verkenning kun je dit 'autonome' ontwikkelingen noemen, die we als de 'buitenwereld' beschouwen. Voorbeelden hiervan zijn klimatologische ontwikkelingen en sociaaleconomische ontwikkelingen, zoals economische, maatschappelijke en

demografische ontwikkelingen. Zo hebben bijvoorbeeld demografische ontwikkelingen een invloed op hoeveel (kwetsbare) mensen worden blootgesteld aan hitte (bijv. door vergrijzing). Omdat de ontwikkelingen onzeker zijn, werken we met een bandbreedte op basis van twee contextscenario's. De daaruit voortvloeiende klimaatrisico's zullen dus ook onzeker zijn en een bandbreedte hebben. De bandbreedte van de twee contextscenario's wordt gebruikt om de robuustheid van de beleidsscenario's te toetsen.

Schematische weergave van te hanteren scenario's voor de nationale klimaatrisicoanalyse 2022 – 2026



Figuur 3 Schematische weergave van de scenario's voor de nationale klimaatrisicoanalyse 2022-2026 (Bron: PBL [7])

De invulling van de contextscenario's van PBL is gebaseerd op:

- De KNMI'23-klimaatscenario's [8];
- De Welvaart en Leefomgeving (WLO'25) scenario's van PBL [11] [12] met ontwikkelingen over o.a. demografie, economie, ruimtegebruik;
- De Deltascenario's 2024 [13], voor een doorvertaling van de KNMI-klimaatscenario's naar o.a. secundaire klimaateffecten op het watersysteem
- Ontwikkelingen bij Landbouw-natuurverkenning (PBL 2025 [14])

De twee contextscenario's zijn gebruikt als startpunt voor zowel het adaptatiescenario 'huidig beleid' als de twee adaptatiescenario's met aanvullende beleid (beleidsmaatregelen) voor 'Intensiveren' als 'Transformeren'.

In deze verkenning gaan we uit van de zichtjaren 2050 en 2100. De contextscenario's bevatten voor de situatie in 2050 zowel klimaat en water/klimaat gerelateerde ontwikkelingen alsook socio-economische ontwikkelingen. Voor de situatie in 2100 zijn de contextscenario's alleen uitgewerkt voor klimaat en water/klimaat gerelateerde ontwikkelingen. Een groot verschil tussen de beide contextscenario's is dat met name de aan klimaat gerelateerde veranderingen bij het 'Sterk risicoverhogend scenario' blijven doorgaan na 2050, terwijl er bij 'Beperkt risicoverhogend scenario' veelal sprake is van een stabilisatie tussen 2050 en 2100. Hieronder zijn de belangrijkste punten overgenomen uit de beschrijvingen van het PBL voor dit onderzoek.

2.1.1.1 Klimatologische ontwikkelingen

De klimatologische ontwikkelingen zijn gebaseerd op de KNMI'23 klimaatscenario's voor Nederland [8]. Deze klimaatscenario's bevatten de laatste inzichten en vervangen de klimaatscenario's uit 2014. De mate waarin ons klimaat zal veranderen, hangt af van de hoeveelheid broeikasgassen die nog zal worden uitgestoten en de gevoeligheid van het klimaatsysteem. Afgeleid van wereldwijde klimaatprojecties, schetsen de KNMI'23-klimaatscenario's het toekomstige klimaat in Nederland voor 2050 en 2100, en geven een indicatie voor de mogelijke zeespiegelstijging in 2150. De KNMI'23-scenario's tellen vier scenario's, opgespannen langs de assen 'mondiale hoogte van broeikasgasemissies', en de 'mate van droge zomers/natte winters'.

Er worden twee typen uitstootscenario's onderscheiden:

1. Hoge uitstootscenario (aangeduid met hoofdletter 'H') waarin de uitstoot sterk toeneemt tot 2080 en daarna afvlakt. De mondiale opwarming rond 2100 wordt hierbij ingeschat op 4,9°C.
2. Lage uitstootscenario (aangeduid met hoofdletter 'L') waarin de uitstoot snel wordt verminderd en broeikasgassen worden verwijderd uit de atmosfeer, in lijn met het Klimaatakkoord van Parijs om de mondiale opwarming tot ruim onder de 2°C te houden. De mondiale opwarming rond 2100 is dan 1,7°C.

Het KNMI heeft gekozen voor een grote bandbreedte in uitstootscenario's om de gevolgen van internationale keuzes in klimaatbeleid zo helder mogelijk te maken, en om nationaal een goede risicoafweging te kunnen maken van de mogelijke gevolgen van klimaatverandering. De toekomstige klimaatverandering ontwikkelt zich waarschijnlijk binnen deze bandbreedte.

Verdere opwarming betekent hoe dan ook dat de Nederlandse zomers droger en de winters natter worden. Voor de mate waarin dit optreedt geven klimaatmodellen verschillende uitkomsten. Daarom onderscheidt het KNMI per uitstootscenario twee varianten:

1. Een 'nat' scenario (aangeduid met de letter 'n') waarin de winters sterk vernatten en de zomers licht verdrogen.
2. Een 'droog' scenario (aangeduid met de letter 'd') waarin de winters licht vernatten en de zomers sterk verdrogen.

Voor de PBL-klimaatrisicoanalyse zijn twee van de vier scenario's gekozen. Als basis voor het contextscenario 'Beperkt risicoverhogend' kiezen wij het Ln scenario (=lage klimaatverandering, natte omstandigheid), voor het contextscenario 'Sterk risicoverhogend' kiezen we 'Hd' (hoge klimaatverandering, droge omstandigheden). Daarmee gebruiken we de grootste bandbreedte voor alle klimaatrisico's die te maken hebben met droogte en watertekort. Voor klimaatrisico's die gerelateerd zijn aan natte omstandigheden, zoals wateroverlast en water-veiligheid (en deels waterkwaliteit), nemen we ook relevante informatie mee uit het Hn scenario (hoge klimaatverandering, natte omstandigheid). Dit doen we om ook voor deze risico's het sterkst risicoverhogende klimaatscenario te gebruiken. De KNMI'23-klimaatscenario's bevatten allerlei klimatologische parameters, inclusief frequentie en intensiteit en klimaatextremen zoals hitte en piekneerslag, zie Figuur 4.

Toename van extremen in het toekomstig klimaat van Nederland



Figuur 4 Extremen in 2100 (Bron: KNMI'23, figuur 3 uit [8]).

2.1.1.2 Demografische, socio-economische en technologische ontwikkelingen

In de contextscenario's gaat het – naast de klimatologische ontwikkelingen – ook om demografische en economische ontwikkelingen en hoe die bijvoorbeeld de vraag naar woningen of energie bepalen, maar niet waar of in welke vorm die woningen dan gebouwd kunnen/mogen worden, en welke vorm van energieproductie de energievraag gaat invullen. De contextscenario's zijn zo 'autonoom en beleidsarm' mogelijk gehouden. Wel worden hier kwalitatief (voor zover bekend) belangrijke technische en sociale innovaties en ontwikkelingen benoemd om hiervan de klimaatrisico's ook in beeld te krijgen.

Bij de invulling van demografische en socio-economische ontwikkelingen is zoveel mogelijk aangesloten bij de informatie uit andere verkenningen, zoals de Welvaart en Leefomgeving studie (WLO'25) van PBL [11]. In onderstaande tabel zijn de relevante gegevens voor de sector ICT opgenomen, naast algemene parameters over demografisch en economisch ontwikkelingen (Bevolking, Economie) en over de energiesector door de sterke afhankelijkheid van de sector ICT van betrouwbare en duurzame energie (elektriciteit).

Sector/onderwerp	Aspecten	Huidig/ referentie 2021	Beperkt risico- verhogend	Sterk risico- verhogend	Ref.
Bevolking	Omvang Bevolkingsgroei (miljoen)	17,5	18,2	21	WLO'25
	Leeftijdsopbouw (%65+)	19,8%	24%	26%	WLO'25
	Leeftijdsopbouw (%80+)				
	% Mensen in steden	32,7%	36,0%	36,0%	WLO'25
Economie	BNP	100	+16%	+87%	WLO'25
Energie	Energievraag		Huidig	Toename	
	Energiemix		Kwalitatief (zie tekst)	Kwalitatief (zie tekst)	
	Elektrificatie, toename elektriciteitsvraag		Toename	Sterke toename	
	Energie- infrastructuur, Bijv. masten, ook op zee		Toename	Sterke toename	
	Verwevenheid andere sectoren		Toename	Sterke toename	
ICT	Digitalisering, ICT vraag		Sterke Toename	Zeer sterke toename	
	ICT infrastructuur		Toename	Sterke toename	
	Verwevenheid andere sectoren		Sterke toename	Zeer sterke toename	

2.1.1.3 Schets contextscenario 'Beperkt risicoverhogend'

Het PBL heeft een verhalende schets gegeven van de invulling van het contextscenario 'beperkt risicoverhogend'. De exacte invulling van de verschillende klimatologische ontwikkelingen en aspecten is beschreven in een apart document en is hier niet opgenomen. Hieronder zijn de relevante aspecten voor dit scenario en de sector ICT overgenomen.

Klimatologische ontwikkelingen

In dit scenario blijft de klimaatverandering voor Nederland beperkt, overeenkomstig het Ln scenario (lage klimaatverandering, natte omstandigheid) van de KNMI'23-scenario's, met name voor de periode na 2050 d.w.z. geen of kleine extra verandering t.o.v. 2050. Zo heeft Nederland in 2050 volgens dit scenario een klimaat dat jaargemiddeld 0.9°C warmer is dan in de referentieperiode (1991-2020) en blijft dit gemiddelde stabiel in de decennia tot 2100. Er valt 3% meer neerslag op jaarbasis, waarbij zomers mogelijk 2% droger worden en de winters 5% natter. De klimatologische veranderingen in (inter)nationale stroomgebieden (met name groter neerslagtekort in zomer) zorgen voor meer variabele rivierafvoeren (c.q. meer in winter, minder in zomer). De zeespiegel ligt naar verwachting in dit scenario in 2050

ongeveer 24 cm hoger dan nu, en zal daarna nog doorstijgen tot 44 cm in 2100. De zeespiegel heeft een langere periode nodig om te stabiliseren. Ondanks deze beperkte zeespiegelstijging zal de verzilting in West-Nederland toch toenemen door minder neerslag, meer grondwateronttrekking en lagere rivierafvoeren. Ook weersextremen nemen beperkt toe. Vooral de klimatologische veranderingen (met name groter neerslagtekort in zomer) en meer variabele rivierafvoeren (c.q. meer in winter, minder in zomer) zorgen ervoor dat veel klimaat gerelateerde wateropgaven ook in “Beperkt risicoverhogend” zullen toenemen.

Demografisch en economisch

De bevolking groeit in eerste instantie maar zal na 2040 dalen tot 18,2 miljoen mensen in 2050 (vergelijkbaar aantal inwoners als nu) (WLO'25 [11]). De economische groei is in deze periode tot 2050 gematigd. Tot 2050 is de verwachte jaarlijkse groei gemiddeld 0,5% per jaar, wat dan in 2050 neerkomt op een totale groei van 16% ten opzichte van 2021. De verwachte groei is laag, onder meer beperkt door beperkte innovatie, waardoor er minder mensen in Nederland komen werken.

Energie

Door de aanvankelijke toenemende bevolking zal de vraag naar energie stijgen, al zal dit beperkt zijn omdat de energietransitie gepaard gaat met energiebesparende maatregelen. Er zullen ook andere maatregelen worden genomen om zoveel mogelijk te voldoen aan klimaatneutraliteit. Het energiesysteem zal bestaan uit meerdere bronnen en de daarbij horende infrastructuur: elektriciteit uit voornamelijk hernieuwbare bronnen (zon, wind, water), waterstof, kernenergie, opslag, Carbon Capture and Storage (CCS), etc. De vraag naar elektriciteit zal toenemen, vanwege elektrificatie van bijv. warmte/koeling, transportmobiliteit en een toename van de ICT. Infrastructuur van energie raakt steeds meer verweven met andere infrastructuren zoals ICT (en vice versa).

ICT

Binnen dit scenario is er sprake van een sterke toename van digitalisering en de bijbehorende vraag naar ICT, en een sterke toename van de verwevenheid van de sector ICT met andere sectoren. De groei van de digitale infrastructuur tot 2050 in Nederland kent een toename, met name door toename van glasvezelaansluitingen, meer opstelpunten voor mobiele netwerken en een toename in colocatie en hyperscale datacenters, voor nieuwe toepassingen. Dit betekent ook dat er specifieke aandacht nodig is voor de gevolgen van klimaatrisico's op de digitale infrastructuur en voor maatregelen om de weerbaarheid binnen de digitale infrastructuur zelf en het gebruik door sectoren te verhogen.

2.1.1.4 Schets contextscenario ‘Sterk risicoverhogend’

Deze paragraaf geeft een verhalende schets van de invulling van het contextscenario ‘sterk risicoverhogend’.

Klimatologische ontwikkelingen

Het contextscenario ‘sterk risicoverhogend’ kent extremere ontwikkelingen die de klimaatrisico's beïnvloeden, overeenkomstig het Hd scenario (hoge klimaatverandering, droge omstandigheden) vanuit de KNMI'23-scenario's. Er worden wel maatregelen genomen om de uitstoot van broeikasgassen te verminderen, maar niet genoeg om klimaatverandering sterk te beperken. Hierdoor, in combinatie met een sterke reactie van het klimaatsysteem, neemt de temperatuur snel toe.

Aanvullend hierop nemen wij voor waterveiligheid en wateroverlast specifieke informatie mee uit het Hn scenario (hoge klimaatverandering, natte omstandigheden) van KNMI'23 [8]. Dit combineren is mogelijk omdat de PBL-studie naar risico's kijkt, niet zozeer naar consistentie. Door beperkte inspanningen op het gebied van mitigatie zet de klimaatverandering substantieel door, met een jaargemiddelde temperatuur die in 2050 en 2100 respectievelijk 1.6°C en 4.4°C hoger ligt dan in referentieperiode (1991-2020). Dit warmere klimaat gaat samen met meer extreme zomers: Het is de verwachting dat er rond 2100 in de Bilt 35 tropische dagen (=max temperatuur > 30°C) zijn in plaats van gemiddeld vijf nu, Maastricht 52 dagen vergeleken met 8 dagen nu. Elk jaar kan ergens in Nederland de 40°C worden aangetikt worden en is 50°C in de stad niet meer uit te sluiten. De extreme zomer van 2019 zou in 2100 een veel langere hittegolf kunnen zijn. Tropische nachten (met name relevant voor gezondheid), kunnen in 2050 wel tot drie keer vaker voorkomen en in 2100 wel tot 19 keer, terwijl ze nu nog heel zeldzaam zijn. De zomers worden veel droger door toenemende verdamping en minder neerslag, waarbij extreme buien in frequentie en intensiteit juist toenemen. De luchtvochtigheid neemt dan ook substantieel af.

Hierdoor zal naar verwachting het gemiddelde jaarlijkse neerslagtekort flink toenemen (met 79% tot 2100), en hebben zowel Maas als Rijn in de zomer vaker te maken met extreme lage afvoeren. Tegelijk kunnen door een grote variabiliteit de maximale afvoeren van beide rivieren ook toenemen (20-30% in 2100). De zeespiegel zal sneller stijgen, vooral na 2050, met tot 14 mm per jaar in 2100 (factor 10 hoger dan nu). Dit leidt ook tot een toename van de verzilting, zowel in hoeveelheid als in oppervlak.

Demografisch en economisch

De bevolkingsomvang neemt toe tot bijna 21 miljoen mensen in 2050, mede door migratie naar Nederland. Ook de economie blijft substantieel groeien. In de periode tot 2050 wordt uitgegaan van een jaarlijkse groei van 2,1% per jaar, wat dan in 2050 neerkomt op een totale groei van 87% ten opzichte van 2021. Dit leidt naar verwachting tot meer vervoer van mens en goederen.

Energie

Het energiesysteem zal bestaan uit vele bronnen en bijbehorende infrastructuur: elektriciteit uit voornamelijk hernieuwbare bronnen (zon, wind, water), waterstof, kernenergie, opslag, Carbon Capture and Storage (CCS), maar vanwege beperktere mitigatiemaatregelen ook nog elementen van huidige energiesysteem gas en olie.

ICT

Binnen dit scenario is er sprake van een zeer sterke toename van digitalisering en de bijbehorende vraag naar ICT, en een zeer sterke toename van de verwevenheid van de sector ICT met andere sectoren. De groei van de digitale infrastructuur tot 2050 in Nederland kent een sterke toename, met name door toename van glasvezelaansluitingen, meer opstelpunten voor mobiele netwerken en een toename in colocatie en hyperscale datacenters, voor nieuwe toepassingen. Dit betekent dat er extra aandacht nodig is voor de gevolgen van klimaatrisico's op de digitale infrastructuur en voor maatregelen om de weerbaarheid binnen de digitale infrastructuur zelf en het gebruik door sectoren te verhogen.

2.1.2 Adaptatiescenario's

In de analyse is gebruik gemaakt van drie adaptatiescenario's:

1. *Huidige beleid*: Het eerste adaptatiescenario omvat het *huidige beleid en -maatregelen*: In dit scenario wordt het huidige adaptatiebeleid doorgetrokken naar de toekomst. Hierin nemen we alleen beleid mee dat vastgesteld, gefinancierd en geïnstrumenteerd is.
De klimaatrisico's die, in combinatie met de contextscenario's, het resultaat zijn van dit scenario, geven aan welke opgaven er over blijven die geadresseerd moeten worden met aanvullend adaptatiebeleid en -maatregelen: de twee aanvullende adaptatiescenario's met beleidsmaatregelen om klimaatrisico's te verminderen.

We gebruiken twee aanvullende toekomstige adaptatiescenario's:

2. *Transformeren*: dit scenario heeft een ruimtelijke focus. We gaan er in dit scenario van uit dat er bij ontwikkelingen in hoge mate rekening wordt gehouden met het water en de bodem, en we zoeken naar meekoppelkansen en *nature-based solutions*. Dit scenario is meer *transformatief* van aard en draait meer om het verminderen van de *blootstelling* van mensen en objecten aan klimaatverandering; hier speelt dus locatie een belangrijke rol.
3. *Intensiveren*: dit scenario heeft een technische focus: dit scenario is gericht op het doorontwikkelen en intensiveren van het huidige beleid en vooral gericht op oplossingen via technische maatregelen, waarbij we in grote lijnen dezelfde dingen blijven doen op dezelfde locaties, maar de effecten van klimaatverandering zoveel mogelijk verkleinen. Daarmee is dit scenario meer *incrementeel*, *reactief* van aard, en vooral gericht op het beperken van de *gevoeligheid* van mensen en objecten voor klimaatverandering.

2.1.3 Klimaatrisico's 2050-2100

Bij de klimaatrisicoanalyse voor de digitale infrastructuur is eerst een globale analyse uitgevoerd van de grootste risico's op basis van interviews en expert opinies. Dit is beschreven in hoofdstuk 4. Hierbij is gekeken naar de **blootstelling** van de verschillende onderdelen binnen de fysieke, digitale infrastructuur aan de verschillende klimaatdreigingen, waarbij de grootste risico's zijn geïdentificeerd, zie paragraaf 4.3.

Vervolgens is in hoofdstuk 6 en 6 een gedetailleerde analyse uitgevoerd voor deze risico's. Hierbij is in meer detail een analyse gemaakt naar de gevoeligheid, blootstelling en impact en naar de adaptatiecapaciteit vanuit de sector en de overheid, in de periode tot 2050. Bij de adaptatiecapaciteit is gekeken naar adaptatiemogelijkheden vanuit de sector zelf en vanuit de overheid.

2.1.3.1 Definities en begrippen in klimaatrisicoanalyse

Voor de klimaatrisicoanalyse is een factsheet 'toekomstig klimaatrisico bij huidig en toekomstig beleid' van het PBL gebruikt. Hieronder zijn de belangrijkste definities uit deze factsheet beschreven. Deze zijn overgenomen uit [7].

Klimaatdreiging ('hazard', H)

Een klimaatdreiging is gedefinieerd volgens ISO 14091 [15] als: "A potential source of harm". In IPCC AR5 [16] wordt dit gespecificeerd als: "The potential occurrence of a natural or

human-induced physical event or trend or physical impact that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, ecosystems and environmental resources. The term ‘hazard’ refers to climate-related physical events or trends or their physical impacts“ [16]. Een klimaatdreiging is dus het mogelijk optreden van een fysieke, klimaat- of weer-gerelateerd fenomeen met de potentie om schade te veroorzaken. Een klimaatdreiging wordt gekarakteriseerd door de intensiteit, de geografische spreiding en de duur van een klimaatfenomeen, en de waarschijnlijkheid dat het fenomeen optreedt.

Secundaire effecten klimaatdreiging

In deze analyse zijn ook eventuele secundaire effecten die door de klimaatdreiging(en) worden veroorzaakt beschreven (bijv. effecten op het bodem-, water- en luchtsysteem) of die de impact van de klimaatdreiging significant vergroten. Denk hierbij aan bijv. daling grondwaterstand, bodemdaling, erosie. Voor de digitale infrastructuur zijn er enkel secundaire effecten ten gevolge van watergebruik voor koeling tijdens langdurige droogte, met mogelijke watertekorten, en kunnen omgekeerd watertekorten leiden tot beperkingen op (drink)watergebruik voor koeling van datacenters.

Blootstelling (‘exposure’, E)

Blootstelling is gedefinieerd volgens IPCC AR5 als: “the presence of people, livelihoods, species or ecosystems, environmental functions, services, and resources, infrastructure, or economic, social, or cultural assets in places and settings that could be adversely affected” [16]. Blootstelling betreft externe factoren, zoals geografische en ruimtelijke positie, kwaliteit van de leefomgeving of klimaat gerelateerde infectiebronnen. De omvang van het gebied dat met een klimaatdreiging te maken krijgt en de inwonersaantallen, bevolkingsdichtheid of economische, sociale of culturele waarde van de bebouwing bepalen onder andere de mate van blootstelling.

Kwetsbaarheid (‘vulnerability’, V)

Kwetsbaarheid heeft als definitie in IPCC AR5: “the propensity or predisposition to be adversely affected. Vulnerability encompasses a variety of concepts and elements including sensitivity or susceptibility to harm and lack of capacity to cope and adapt” [16].

Kwetsbaarheid betekent de neiging van een systeem om negatief beïnvloed te worden door een klimaatdreiging. Kwetsbaarheid betreft interne eigenschappen van het getroffen systeem zelf. Kwetsbaarheid is een functie van de gevoeligheid (S = Sensitivity) voor een klimaatdreiging en de adaptatiecapaciteit (AC = Adaptive Capacity) om deze dreiging op voorhand (preventieve adaptatie) of de gevolgen daarvan (reactieve adaptatie) het hoofd te bieden.

Gevoeligheid (‘sensitivity’)

Gevoeligheid is volgens IPCC AR5 gedefinieerd als: “The degree to which a system or species is affected, either adversely or beneficially, by climate variability or change” [16]. Gevoeligheid is de mate waarin een systeem negatief of positief beïnvloed wordt door klimaatverandering.

Adaptatiecapaciteit (‘adaptive capacity’)

Adaptatiecapaciteit is gedefinieerd in IPCC AR5 als: “the ability of systems, institutions, humans, and other organisms to adjust to potential damage, to take advantage of opportunities, or to respond to consequences” [16]. Adaptatiecapaciteit is het vermogen van

systemen, instituties, mensen of organismen om zich aan te passen aan mogelijke schade, kansen te benutten of te reageren op gevolgen. Adaptatie is het proces van aanpassing aan werkelijke of mogelijke klimaatimpacts, zoals beschreven in ISO 14091 [15].

Adaptatiecapaciteit is een complex begrip met veel aspecten. Adaptatiecapaciteit gaat om bewustzijn van en aandacht voor het risico in de betreffende beleidsvelden, en de aanwezigheid van plannen voor adaptatie, flexibiliteit en de omloopsnelheid en/of levensduur van investeringen in het systeem dat moet worden aangepast door technische, organisatorische, bestuurlijke, financiële en politieke factoren.

Adaptatie

Adaptatie is gedefinieerd in IPCC AR5 als: “the process of adjustment to actual or expected climate and its effects in order to moderate or avoid harm or exploit beneficial opportunities” [16]. Adaptatie is het proces van aanpassing aan huidige of toekomstige klimaateffecten om schade te beperken of voorkomen en kansen te benutten. Op basis van de klimaatrisico's en adaptatiecapaciteit kunnen adaptatiemaatregelen en beleid voor adaptatie worden ontwikkeld. Adaptatie kan worden onderverdeeld in enerzijds autonome/spontane en anderzijds geplande adaptatie. Autonome adaptatiecapaciteit is het vermogen van natuurlijke en marktsystemen om zichzelf ‘autonoom’, dat wil zeggen zonder hierop gericht overheidsbeleid, aan te passen aan klimaatverandering. Voorbeelden van autonome adaptatie zijn migratie van soorten, aanschaf van beregeningsinstallaties en airconditioners, overgaan op droogte-resistentere gewassen in de landbouw. Geplande adaptatie is het resultaat van doelbewust overheidsbeleid, gebaseerd op het bewustzijn dat omstandigheden veranderen en dat daarom actie noodzakelijk is. Het onderscheid tussen autonome en geplande adaptatie is niet altijd goed te maken. Adaptatie kan ook worden ingedeeld naar preventieve en reactieve adaptatie. Preventieve adaptatie is het nemen van maatregelen vooraf om klimaatrisico's te verkleinen, gericht op het verminderen van zowel de blootstelling als kwetsbaarheid [2]. Bijvoorbeeld door verhogen van dijken, aanleggen van museumdepots op veilige plekken en organiseren van waarschuwingssystemen. Reactieve adaptatie is het nemen van maatregelen op het moment dat een klimaatgebeurtenis plaatsvindt ter verkleining van de impact. Voorbeelden zijn het tijdig onder de aandacht brengen van het Nationaal hitteplan van het RIVM, een communicatieplan met eenvoudige maatregelen voor risicogroepen bij hitte (of bij een overstroming het plaatsen van zandzakken of evacuatie van een gebied. Onder reactieve adaptatie valt ook het regelen dat na de gebeurtenis de schade vlot wordt hersteld en het gewone leven weer snel op gang komt.

Waarschijnlijkheid ('probability' of 'likelihood')

In IPCC AR5 is de definitie van waarschijnlijkheid: “the chance of a specific outcome occurring, where this might be estimated probabilistically” [16]. Waarschijnlijkheid is de statistische kans of de aannemelijkheid dat een klimaatdreiging en/of een gevolg daarvan optreedt. Of er een risico is en hoe groot die is, hangt af van de aard, omvang, intensiteit en het moment van de klimaatgebeurtenis, in combinatie met de blootstelling en kwetsbaarheid van het systeem. De impact (potentieel negatief gevolg) van een klimaatdreiging kan direct of indirect doorwerken in een systeem (ISO 14091 [15]).

Een risico kan ook berekend worden door de waarschijnlijkheid te vermenigvuldigen met de impact.

Impact

Impact is gedefinieerd in IPCC AR5 als: “effects on natural and human systems of extreme weather and climate events and of climate change. Impacts generally refer to effects on lives,

livelihoods, health, ecosystems, economies, societies, cultures, services and infrastructure due to the interaction of climate changes or hazardous climate events occurring within a specific time period and the vulnerability of an exposed society or system“ [16]. In de context van klimaatverandering is ‘impact’ gedefinieerd als de gevolgen voor natuurlijke en menselijke systemen van extreem weer gebeurtenissen of sluipende klimaatverandering. Dit kunnen gevolgen zijn voor leven en levensonderhoud, gezondheid, ecosystemen, economie, samenleving, cultuur, diensten en infrastructuur. Impact is de invloed op iets dat van waarde wordt gevonden. Een impact is een gevolg van een werkelijke gebeurtenis, in tegenstelling tot een risico, dat een onzekere potentiële gebeurtenis is met gevolg. Impact wordt ook ‘gevolg’ (‘consequence’) genoemd, bijvoorbeeld in de UK’s Third Climate Change Risk Assessment (UK CCRA3 [17]).

Eindrisico

Impacts kunnen het directe gevolg zijn van klimaatgebeurtenissen, of het indirecte gevolg van een keten of ketens van gebeurtenissen (zie bijlage 8 voor de ISO 14091 [15] handreiking voor het opstellen van impactketens). Voor het vergelijken van klimaatrisico’s is het belangrijk om de uiteindelijke impact van zo’n keten te bepalen, gedefinieerd als ‘eindrisico’.

2.1.4 Beleidsboodschappen

Op basis van de klimaatrisicoanalyse bij huidig beleid zijn de opgaven beschreven waarop aanvullend beleid nodig is om de risico’s in de toekomst verder te beperken, zie paragraaf 5.7. Vervolgens zijn deze beleidsopgaven gebruikt om mogelijke maatregelen voor aanvullend beleid op te stellen voor ‘intensiveren’ of ‘transformeren’, zie hoofdstuk 6. De maatregelen zijn gebruikt om opnieuw te bepalen in hoeverre de klimaatrisico’s in 2050 (en 2100) worden verminderd en of er nog restrisico’s zijn. Op basis van deze tweede analyse worden beleidsopties voorgesteld voor de sector ICT, zowel voor de digitale infrastructuur voor generiek gebruik (openbare netwerken) als voor sectorspecifieke digitale infrastructuur.

2.2 Toepassing systematiek sector ICT

Voor de klimaatrisicoanalyse is hieronder beschreven op welke manier dit is toegepast voor de analyse van de sector ICT.

Voor de analyse is de sector ICT beschreven, d.w.z. de digitale infrastructuur in Nederland en de rol binnen Europa. Hierbij is onderscheid gemaakt in de digitale infrastructuur voor generieke of openbare ICT-diensten (zie hoofdstuk 3), en in sectorspecifieke infrastructuur voor bijv. de energiesector, openbare orde en veiligheid, gezondheidszorg (ziekenhuizen) en transport (zie hoofdstuk 7). Binnen de twee **contextscenario’s** (beperkt en sterk risicoverhogend) zijn globaal ook de verwachte toekomstige ontwikkelingen (trends) binnen de digitale infrastructuur beschreven tot 2050. Voor de periode 2050-2100 is onvoldoende duidelijk hoe de fysieke, digitale infrastructuur zich ontwikkelt, binnen Nederland en binnen Europa.

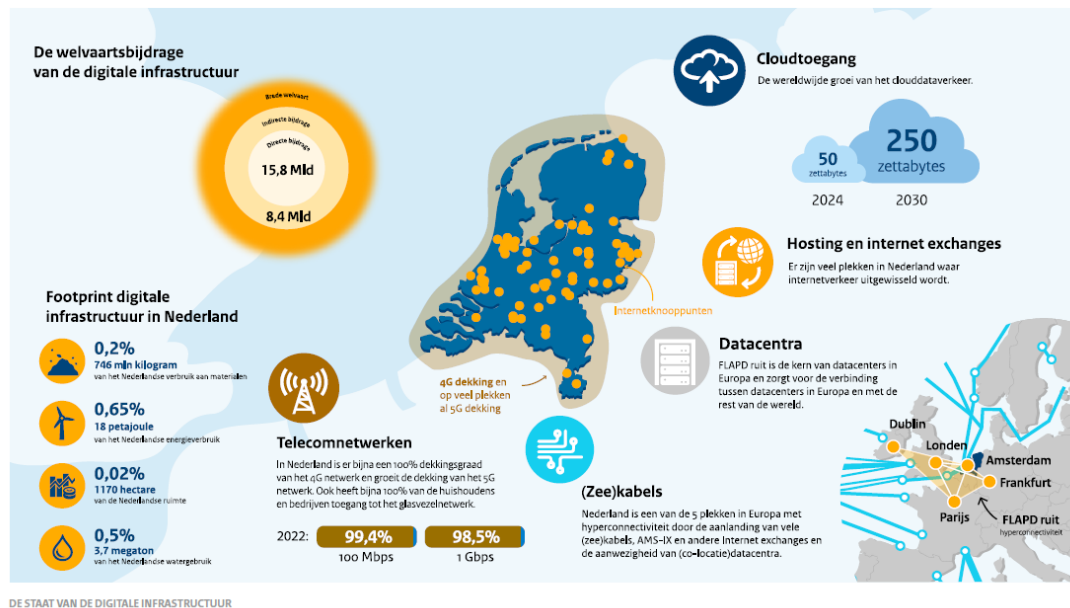
Voor het **adaptatiescenario ‘huidig beleid’** is gekeken naar **geïmplementeerd beleid en huidige wetgeving** t.a.v. klimaatrisico’s. Hierbij is gekeken naar verschillende beleidsthema’s zoals economische beleid, ruimtelijk beleid, duurzaamheid en beleid ten aanzien van de weerbaarheid van vitale digitale infrastructuur in Nederland. Voor de

wetgeving is gekeken naar huidige wetgeving (zoals de telecommunicatiewet en wetgeving voor bijv. datacenters) en naar wetgeving die op korte termijn verwacht wordt aangezien hiervoor al conceptteksten beschikbaar zijn op basis van Europese richtlijnen, zoals de Cyberbeveiligingswet (Cbw) voor de NIS2-richtlijn en de Wet weerbaarheid kritieke entiteiten (Wwke) voor de CER-richtlijn. Voor de twee adaptatiescenario's met aanvullend beleid (transformeren en intensiveren) zijn mogelijke aanvullende beleidsmaatregelen beschreven.

3 Digitale infrastructuur in Nederland

3.1 Opdeling van de digitale infrastructuur

Datacenters en netwerkknooppunten zijn via glasvezelkabels over land en zee onderling verbonden en vormen een belangrijke basis voor het internet. Ook datacenters van globale cloud-providers, zoals Amazon, Microsoft en Google, zijn onderling verbonden voor clouddiensten. In de afgelopen decennia heeft onze digitale infrastructuur zich voortvarend ontwikkeld. Daarbij is Nederland niet alleen binnen Europa, maar ook wereldwijd al jarenlang één van de koplopers. Europees gezien hoort Nederland bij de top van lidstaten met de beste digitale connectiviteit (zie bijv. figuur 14 in [18]). De digitale infrastructuur is een nauw verweven ecosysteem dat uit veel schakels bestaat. Al deze schakels moeten goed functioneren. Zo zorgen ze samen voor een hoogwaardige, betrouwbare, veilige en toegankelijke digitale infrastructuur binnen Nederland en naar de rest van de wereld.



Figuur 5 Overzicht van de staat van de digitale infrastructuur (Bron: [19])

We beschouwen de digitale infrastructuur als het geheel aan schakels dat de eindgebruiker in staat stelt om toegang te krijgen tot digitale content en applicaties. We gebruiken de opdeling zoals gebruikt in het rapport van het Ministerie van EZK “De staat van de digitale infrastructuur” [19] met de volgende vijf fysieke componenten:

1. **Telecomnetwerken:** vaste en mobiele netwerken in Nederland van bijv. KPN, Odido en VodafoneZiggo, en kleinere aanbieders. Telecomnetwerken bestaan uit

verschillende fysieke componenten, zoals datakabels (glasvezel, koper en coax), opstelpunten (zendmasten en opstelpunten op gebouwen), technische gebouwen zoals lokale straatkasten in wijken, kasten bij zendmasten, en lokale, regionale en nationale (core) locaties met actieve netwerkapparatuur.

2. **(Zee)kabels:** naast de kabels in de nationale telecomnetwerken zijn er ook internationale kabelverbindingen onder land en zee.
3. **Datacenters:** datacenters zijn het motorblok van de digitale infrastructuur. Hier staan dag en nacht servers te zoemen. Datacenters zijn in de kern gebouwen waar servers staan die op afstand bewerkingen doen en informatie opslaan voor consumenten, bedrijven en overheden.
4. **Hosting en internet exchanges:** internet exchanges of internetknooppunten zijn locaties waar netwerken van verschillende telecomaandieners onderling zijn verbonden en verkeer wordt uitgewisseld. Hosting is een specifiek type datacenterdienst waarbij content of applicaties via het internet wordt ontsloten.
5. **Cloudtoegang:** ook Cloud hosting is een specifieke vorm van dienstverlening die vanuit grote datacenters (hyperscale) worden geboden, bijv. door globale aanbieders zoals Amazon (Amazon Web Services), Google (Google Cloud) en Microsoft (Azure).

De digitale infrastructuur vormt de basis voor het leveren van digitale diensten door commerciële aanbieders aan consumenten, zakelijke gebruikers en overheden. Er is dus sprake van een private sector, die digitale diensten leveren, bijv. door telecomaandieners zoals KPN, Odido of VodafoneZiggo voor vaste en mobiele telefonie, internettoegang en netwerkdiensten, door datacenterproviders en door cloud-providers zoals Amazon, Microsoft en Google. Daarnaast beschikken overheid en bedrijven ook over eigen private infrastructuur. Zo zijn er besloten netwerken zoals het C2000-netwerk voor Openbare Orde en Veiligheid (OOV), het NAFIN-netwerk van Defensie, maritieme netwerken op zee en in havens en netwerken op en rondom vliegvelden zoals Schiphol. Ook hebben individuele bedrijven en organisaties eigen ICT-netwerken op en tussen locaties, zoals kantoren, meldkamers, etc., die geheel onder de verantwoordelijkheid van deze organisaties vallen.

De Nederlandse Rijksoverheid heeft een belangrijke rol in de wetgeving voor de digitale infrastructuur, die meer en meer vanuit de Europese Commissie wordt opgesteld via Europese wetgeving zoals Digital Market Act (DMA) en Digital Services Act (DSA). Ook zijn er Europese richtlijnen die in nationale wetgeving zijn of (worden) omgezet, zoals de European Electronic Communications Code (EECC) richtlijn voor de Telecommunicatiewet (Tw), de Network and Information Security 2 richtlijn (NIS2) voor de Cyberbeveiligingswet (Cbw) en de Critical Entities Resilience (CER) richtlijn voor de Wet weerbaarheid kritieke entiteiten (Wwke).

3.1.1 Masten

Zendmasten en andere opstelpunten (bijv. op hoge gebouwen) zijn een belangrijk onderdeel in 'netwerken voor radiocommunicatie', met verschillende communicatiedoeleinden zoals mobiele netwerken, C2000 en radionetwerken voor radio en televisie. In deze masten of opstelpunten worden antennes geplaatst in de mast en radioapparatuur (in de mast of in een kast onder bij de mast). De masten zijn via glasvezelverbindingen aangesloten op het mobiele netwerk en zijn voorzien van elektriciteit. Naast aparte masten worden er ook antennes en actieve apparatuur op hoge gebouwen geplaatst of in elektriciteitsmasten. De belangrijkste landelijke netwerken zijn de drie mobiele netwerken van KPN, Odido en

VodafoneZiggo, het C2000-netwerk en de netwerken voor radio en televisie. Verder zijn er nog andere besloten (lokale) netwerken voor overige communicatie, zoals voor maritieme communicatie en luchtvaartcommunicatie rondom vliegvelden en aanvliegroutes. Wanneer zich een crisissituatie voordoet tijdens of vanwege extreem weer, kunnen verstoorde communicatiediensten bijzonder gevaarlijk zijn. Het is van levensbelang dat diensten voor het ontvangen van cruciale informatie en het contact kunnen opnemen met hulpdiensten blijft werken. [20] In aanvulling op het contextscenario 2050 is hieronder beschreven welke ontwikkelingen relevant zijn in de periode tot 2050 voor de verschillende netwerken.

Mobiele netwerken: In Nederland zijn er momenteel drie landelijke mobiele netwerken van KPN, VodafoneZiggo en Odido (voorheen T-Mobile). Deze worden voortdurend aangepast aan de nieuwste technologie. Momenteel zijn 4G en 5G de dominante technologieën en wordt 2G en 3G in de komende jaren uitgefaseerd. Iedere 10 jaar is er een nieuwe generatie netwerken, en in 2050 zullen naar verwachting 6G en 7G de dominante technologieën zijn. Deze nieuwe generaties van netwerken zullen hogere datasnelheden ondersteunen, door meer spectrum, efficiënter gebruik van spectrum en meer opstelpunten. Opstelpunten worden ook meer en meer gedeeld door verschillende mobiele netwerk operators, waarbij ze zelf hun antennes en radioapparatuur in dezelfde masten en andere opstelpunten kunnen installeren. Tot 2030 wordt een lichte afname van het aantal mobiele abonnees in West-Europa verwacht, van 497 in 2024 naar 490 miljoen in 2030 [21]. Er is een duidelijke toename van 5G abonnees van 42% in 2024 naar 91% in 2030 en hiermee groeit ook het dataverkeer per abonnee, waardoor het totale dataverkeer sterk zal toenemen, met een jaarlijkse groei van maximaal 20%. Met 5G neemt ook het energieverbruik van mobiele netwerken (70% radionetwerk, 30% kernnetwerk) en randapparatuur sterk toe, van 230 TWh per jaar in 2020 naar 597 TWh in 2030 [22]. In 6G is er wel hernieuwd aandacht voor energie-efficiëntie, maar het is onduidelijk of dit zal leiden tot vermindering van energiegebruik van randapparatuur en radionetwerken na 2030.

C2000: Het C2000-netwerk van de Rijksoverheid wordt sinds 2004 gebruikt en is een besloten communicatienetwerk met eigen radiomasten (500+) voor communicatie tussen hulpverleners (meer dan 80.000) onderling en met meldkamers [23]. C2000 is gebaseerd op TETRA-technologie, en met name geschikt voor spraakverbindingen (portofonie) en alarmering. C2000 heeft zeer beperkte mogelijkheden om data te versturen, hiervoor maken hulpverleners nu gebruik van mobiele 4G- en 5G-netwerken. De verwachting is dat C2000 na 2030 vervangen zal zijn door missiekritische communicatie via één of meerdere openbare mobiele netwerken. Hiermee wordt het belang van goed werkende mobiele netwerken groter, met aanvullende maatregelen voor bereik en beschikbaarheid bij uitval.

Radio, televisie en overige netwerken (maritieme communicatie en luchtvaartcommunicatie): deze netwerken zijn globaal meegenomen in de analyse. Algemeen geldt dat de beschikbaarheid van lokale netwerken voor maritieme en luchtvaartcommunicatie zeer hoog dient te zijn en incidentele verstoringen door uitval van apparatuur in deze lokale, besloten netten tot een minimum beperkt moeten zijn. Een mogelijke toename van storingen door klimaatrisico's (hitte) zal hierbij door de verantwoordelijke organisatie moeten worden beschouwd. Generieke netwerkapparatuur in deze netwerken zal typisch iedere 5-10 jaar worden vervangen, specifieke apparatuur 10-20 jaar, en bij structurele problemen zal men besluiten om verbeterde apparatuur te gebruiken die minder gevoelig is voor bijv. hitte, of aanvullende maatregelen nemen voor (verbeterde) koeling.

3.1.2 Datacenters

Datacenters vormen een cruciale schakel in de digitale infrastructuur en zijn afhankelijk van stabiele koelsystemen om oververhitting te voorkomen. De opwarming van het klimaat leidt tot een toenemend aantal (extreem) warme dagen en langere perioden van droogte, wat de werking van deze systemen onder druk zet. Dit kan resulteren in een hogere energievraag, verhoogde kans op storingen in de koeling en beperkingen in de beschikbaarheid van water voor koeling. Nederland kent een groeiende datacentermarkt, met zowel colocatie-datacenters als hyperscale datacenters van internationale techbedrijven voor cloudtoegang zoals Google, Microsoft en Amazon. In Nederland zijn twee locaties aangewezen voor hyperscale datacenters: in Groningen (Eemshaven) en in Noord-Holland (Middenmeer) met hyperscale datacenters van Google en Microsoft.

Koeling speelt een essentiële rol in het handhaven van operationele stabiliteit, waarbij water- en luchtkoeling de meest gebruikte technieken zijn. Echter, het gebruik van drinkwater voor koeling staat steeds vaker ter discussie, zeker in tijden van droogte.

Deze analyse richt zich daarom op de volgende potentiële klimaatrisico's voor datacenters:

3.2 Hoge mate van beschikbaarheid

De digitale infrastructuur in Nederland kenmerkt zich door een hoge mate van betrouwbaarheid en stabiliteit [24] door het gebruik van redundantie, waardoor de digitale infrastructuur bestand is tegen lokale, technische verstoringen. Het redundantieniveau wordt bepaald door het aantal back-up verbindingen en/of componenten ter voorkoming van uitval of verstoring van de dienst als gevolg van uitval of verstoring van een verbinding of component. De minimale redundantie voor belangrijke componenten en/of verbindingen is $N+1$. In deze formule representeert N het minimaal aantal benodigde verbindingen of componenten dat noodzakelijk is voor het leveren van de dienst. De $+1$ houdt in dat het netwerk zo geconfigureerd is dat, als één willekeurig component, server of netwerkverbinding uitvalt, dit niet tot verstoring leidt. Deze redundantie wordt op verschillende manieren toegepast, bijv. in losse systemen met redundante voedingen, CPU, geheugen en netwerkkaarten, door gebruik van meerdere (back-up) systemen, locaties, glasvezelverbindingen en telecomaانبieders, etc. Hogere redundantieniveaus dan $N+1$ zijn uiteraard ook mogelijk en worden, afhankelijk van de (financiële) risico's, ook veelvuldig toegepast.

De kern van het telecomnetwerk van iedere telecom operator is typisch zodanig ontworpen dat het een meervoudige redundantie heeft van typisch $N+2$ of $N+3$. De mate van maatregelen is veelal afhankelijk van het aantal eindgebruikers (100.000'en tot miljoenen) of percentage van eindgebruikers (1-10%, 10-100%) dat geraakt kan worden bij een verstoring. Globale cloud providers zoals Amazon, Microsoft en Google, hanteren in hun wereldwijde Cloud netwerken veelal nog hogere redundantieniveaus van $N+4$ of zelfs $N+5$ op verbindingen en locaties, om te voorkomen dat cloud diensten niet werken of data van klanten verloren kan gaan in situaties als meerdere verstoringen gelijktijdig optreden. De hoge redundantieniveaus in vitale en centrale onderdelen van telecomnetwerken zijn een belangrijk kenmerk van de digitale infrastructuur. Daarnaast kunnen met name bedrijven en organisaties zich weerbaarder maken voor uitval bij één partij door gelijktijdig gebruik te maken van verschillende aanbieders: bijv. meerdere mobiele netwerk operators in

Nederland, verschillende aanbieders van colocatie datacenters of van meerdere cloud providers, zoals Amazon, Microsoft en Google.

3.3 Trends

Binnen de digitale sector zijn er drie belangrijke trends te onderkennen:

- Het streven naar duurzame digitalisering en de transitie naar klimaatneutraal opereren binnen de digitale sector als geheel en in belangrijke mate ook voor (hyperscale) datacenters. Dit is vastgelegd in het “Actieplan Duurzame Digitalisering” [25] van juni 2024, waarin acties zijn beschreven om de digitale sector te verduurzamen, juni 2024). Het actieplan is in de eerste fase gericht op datacenters binnen de digitale infrastructuur. Datacenters zorgen voor 38% van directe (scope 1) en indirecte (scope 2) emissies en dit biedt de grootste kansen voor verdere verduurzaming. In actielijn 1a van het plan zijn nieuwe en lopende acties beschreven voor verduurzaming van datacenters, zoals een verkenning naar randvoorwaarden en standaarden voor vestigingslocaties van datacenters in Nederland, cofinanciering van Digital Europe projecten voor duurzame datacenters en cofinanciering van het IPCEI CIS project ‘Modular & Integrated Sustainable Datacenter (MISD)’;
- Een toenemende aandacht voor de weerbaarheid van de digitale infrastructuur als vitale functie, via Europese richtlijnen (CER en NIS2) en nationale wetgeving (Wwke en Cbw) voor het fysieke en digitale domein [26]. Er is een steeds verdere verknoping van de digitale infrastructuur met infrastructuur van beschadigandere sectoren door digitalisering in die andere sectoren. Daarmee wordt de digitale infrastructuur in steeds hogere mate net zo kritiek als het elektriciteitsnet. De nieuwe wetgeving legt meer focus op de vitale functie van de digitale infrastructuur, zowel de openbare als sectorspecifieke ICT-infrastructuur.
- Toegang tot betaalbare satellietcommunicatie voor consumenten en organisaties door nieuwe diensten van bijv. Starlink en Oneweb. Via nieuwe Low Earth Orbit (LEO) satellietconstellaties van deze bedrijven kan gebruik worden gemaakt van satellietcommunicatie via bijv. smart phones in gebieden zonder mobiele dekking of bij uitval van deze netwerken op land bij het optreden van klimaatrisico’s.

Door de transitie naar klimaatneutraal worden nieuwe investeringen gedaan in verbeterde oplossingen t.a.v. stroomvoorziening en verbeterde koeling, waarbij er ook aandacht is voor uitval door klimaatrisico’s. Door het toenemende belang van digitale infrastructuur als vitale functie en aanvullende wetgeving via de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke) komt er meer aandacht voor continuïteit van de digitale infrastructuur bij organisaties en bedrijven. Keteneffecten bij uitval van individuele datacenters zijn moeilijk in te schatten, maar kunnen wel voor grote maatschappelijke ontwrichting zorgen als dit bijv. leidt tot uitval van vitale communicatievoorzieningen, zoals bij de recente grote storing bij AWS op 20 oktober 2025 die impact heeft gehad op veel verschillende diensten wereldwijd.

Naast bovenstaande trends zijn er ook verschillende technologische trends zoals edge computing (kleinere gedistribueerde datacenters in randen van netwerk), AI (andere typen datacenters in AI-factories), en quantum computing (met superkoeling van quantum computers) die een rol kunnen gaan spelen in veranderingen in de digitale infrastructuur en de klimaatrisico’s.

3.3.1 Trend 1: Duurzaamheid en ICT

Binnen de digitale sector is duurzaamheid en energie een belangrijk thema. Datacenters verbruiken meer en meer elektriciteit (o.a. door toename in gebruik van internet, clouddiensten en recent ook AI). Nederlandse en Europese wetgeving en richtlijnen zijn gericht op energiebesparing, efficiënter gebruik van elektriciteit en op besparing in watergebruik, met name voor datacenters. Dit heeft tot gevolg dat de ecologische voetafdruk van de digitale sector minder sterk toeneemt dan de groei van deze sector zou vermoeden. Door de wettelijke verplichtingen rondom duurzaamheid worden nieuwe investeringen gedaan in verbeterde oplossingen t.a.v. CO₂-neutrale stroomvoorziening en betere koeltechnieken, bijv.

- ☐ Vermindering van watergebruik (Water Usage Efficiency, WUE) door andere koeltechnieken en datacenters die bij een hogere temperatuur werken (29 i.p.v. 25 graden);
- ☐ Overstap van drinkwater naar andere waterbronnen voor koeling (opvang van regenwater, gebruik van oppervlaktewater);
- ☐ Vermindering van stroomverbruik door efficiëntie-maatregelen (Power User Efficiency, PUE);
- ☐ Directe investeringen in windmolenparken en zonneparken door hyperscalers.

Een positief bijeffect van deze aanpassingen is dat klimaatrisico's voor datacenters kleiner worden, bijv. omdat nieuwere datacenters bij hogere temperaturen (tot 29 i.p.v. 25°C) kunnen werken zonder waterkoeling, en eventueel bij hogere temperaturen geraakt worden door mogelijke restricties op laagwaardig gebruik van drinkwater voor koeling. Daarnaast zorgt wetgeving op het gebied van duurzaamheid ook dat afnemers van ICT-diensten kijken naar de prestaties op het gebied van duurzaamheid van de verschillende aanbieders in de digitale sector, bijv. bij de keuze van een datacenters aanbieder of cloud dienst. Op gebied van duurzaamheid presteren grote cloud providers in het algemeen beter op PUE en WUE dan kleinere aanbieders van datacenters door hun schaalgrootte en efficiënter gebruik van hun datacenters verspreid over Europa en de wereld.

3.3.2 Trend 2: Vitale digitale infrastructuur

Er ligt een wetsvoorstel [27] voor de Wet weerbaarheid kritieke entiteiten (Wwke) voor implementatie van richtlijn (EU) 2022/2557 (de zogeheten Critical Entities Resilience Directive, CER-richtlijn). Die richtlijn strekt tot het waarborgen van de levering van essentiële diensten in de interne markt, door de weerbaarheid van de aanbieders van deze essentiële diensten (in de richtlijn aangeduid als "kritieke entiteiten") in de lidstaten te versterken. In het wetsvoorstel zijn voor de digitale infrastructuur de volgende kritieke entiteiten opgenomen, met verwijzingen naar de Cbw/NIS2-richtlijn:

- ☐ aanbieders van **internetknooppunten** als bedoeld in artikel 6, onderdeel 18, van de NIS2-richtlijn;
- ☐ **DNS-dienstverleners** als bedoeld in artikel 6, onderdeel 20, van de NIS2-richtlijn, met uitzondering van exploitanten van root-naamservers. In Nederland is dit één partij: de DNS Registry operator voor het .nl domein door SIDN (Stichting Domeinnaam Nederland);
- ☐ registers voor **topleveldomeinnamen** als bedoeld in artikel 6, onderdeel 21, van de NIS2-richtlijn; aanbieders van **cloudcomputingdiensten** als bedoeld in artikel 6, onderdeel 30, van de NIS2-richtlijn;
- ☐ aanbieders van **datacenterdiensten** als bedoeld in artikel 6, onderdeel 31, van de NIS2-richtlijn;

- aanbieders van **netwerken voor content delivery** als bedoeld in artikel 6, onderdeel 32, van de NIS2-richtlijn;
- verleners van **vertrouwensdiensten** als bedoeld in artikel 3, onderdeel 19, van Verordening (EU) nr. 910/201424;
- aanbieders van **openbare elektronische communicatienetwerken** als bedoeld in artikel 2, onderdeel 8, van Richtlijn (EU) 2018/197225;
- aanbieders van **elektronische communicatiediensten** als bedoeld in artikel 2, onderdeel 4, van Richtlijn (EU) 2018/1972, voor zover hun diensten publiek beschikbaar zijn.

Kritieke entiteiten worden t.z.t. door de overheid aangewezen op basis van een aantal criteria (artikel 6 van de Wwke). Het Ministerie van EZ zal dit doen voor de telecomsector ofwel voor aanbieders binnen de digitale infrastructuur. De overheid voert een risicobeoordeling uit en neemt daarbij alle relevante natuurlijke en door de mens veroorzaakte risico's die tot een incident zouden kunnen leiden in aanmerking, waaronder in ieder geval (artikel 9 van de Wwke):

- a) risico's van sectoroverschrijdende of van grensoverschrijdende aard;
- b) ongevallen;
- c) natuurrampen;
- d) noodsituaties op het gebied van de volksgezondheid; en
- e) hybride dreigingen en andere antagonistische dreigingen, waaronder terroristische misdrijven als bedoeld in de Richtlijn (EU) 2017/541.

De kritieke entiteit is daarna wettelijk verplicht om zelf een risicobeoordeling uit te voeren - op basis van de relevante informatie uit de risicobeoordeling van de bevoegde autoriteit van de overheid (artikel 14 van de Wwke) en andere relevante informatiebronnen - en heeft vervolgens een zorgplicht om passende en evenredige technische, beveiligings- en organisatorische maatregelen te treffen om voor haar weerbaarheid te zorgen (artikel 15 van de Wwke). De Wwke richt zich op de weerbaarheid van deze aanbieders in het fysieke domein en betreft nadrukkelijk niet de weerbaarheid in het digitale domein. Klimaatrisico's zijn niet expliciet opgenomen, anders dan natuurrampen (zoals overstromingen).

De beveiliging van de netwerk- en informatiesystemen van kritieke entiteiten wordt geregeld in een andere richtlijn, de NIS2-richtlijn (EU) 2022/2555. Voor de NIS2-richtlijn is een nationaal wetsvoorstel [28] voor de Cyberbeveiligingswet (Cbw) opgesteld. Omdat de digitale veiligheid van onze samenleving en economie steeds vaker onder druk staat, heeft de Europese Unie (EU) de NIS2-richtlijn vastgesteld. Deze richtlijn is de opvolger van de NIS1-richtlijn. De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken. De Cyberbeveiligingswet is – naast de digitale infrastructuur en beheer van ICT-diensten, ook van toepassing op een groot aantal sectoren, zoals energie, vervoer, bankwezen, drinkwater, gezondheidszorg en overheid. Aangewezen entiteiten binnen deze sectoren dienen te voldoen aan de Cbw.

3.3.3 Trend 3: Satellietcommunicatie

Satellietcommunicatie wordt gebruikt voor communicatie en voor plaatsbepaling en tijdsbepaling (GNSS, zoals GPS en Galileo). De klimateffecten op de satellieten zijn beperkt door de locatie van satellieten in de ruimte op 600 tot 36.000 km van de aarde. Een satellietnetwerk bestaat echter ook uit fysieke infrastructuur op land zoals schotelantennes op grondstations, verspreid over verschillende landen in Europa. De grondstations zijn

aangesloten op de vaste datanetwerken op land via glasvezelverbindingen. De klimaatrisico's die leiden tot verstoringen bij grondstations zijn daarmee identiek aan die voor de vaste (technische) locaties op aarde. Satellietcommunicatie is een belangrijk onderdeel in de mix van communicatiemiddelen daar deze veelal beschikbaar blijft, bijvoorbeeld als de fysieke infrastructuur (telecom en elektriciteit) op land (zwaar) is beschadigd en weggefallen bij grote overstromingen of na een orkaan in het Caribisch deel van Nederland. Daarmee is satellietcommunicatie een belangrijke aanvulling in geval van calamiteiten.

4 Klimaatrisico's digitale infrastructuur

4.1 Klimaatdreigingen

Klimaatverandering resulteert in diverse klimaatdreigingen. Klimaatdreigingen bestaan uit zowel geleidelijke veranderingen van het gemiddelde klimaat (bijvoorbeeld gemiddelde opwarming van de aarde) als uit veranderingen van extremen (bijvoorbeeld hittegolven). Een klimaatdreiging wordt gekarakteriseerd door de intensiteit, geografische omvang en duur van een weerfenomeen. De KNMI'23 klimaatscenario's [8] vormen de basis voor de toekomstige klimaatdreigingen. Onderstaande lijst met de vijf klimaatdreigingen is gebruikt in de analyse voor de sector ICT.

1. **Het wordt warmer:** de gemiddelde temperatuur stijgt; vaker warm weer (risico op meer blootstelling aan UV straling); frequentere, langdurigere en heviger hitteperioden; opwarming van bodem, lucht, oppervlaktewater, zeewater; slechtere kwaliteit van bodem, lucht, oppervlaktewater, zeewater; toename verdamping; versnelling bodemdaling.
2. **Het wordt natter:** de gemiddelde jaarneerslag neemt toe, met uitzondering van de zomer; frequentere, langdurigere en heviger piekbuien met risico op lokale wateroverlast en overstromingen; grotere kans op hoogwater in rivieren in winter; frequentere en heviger piekafvoeren in grote en regionale rivieren met risico op overstromingen vanuit rivieren; frequenter hoge waterpeilen in meren; grotere luchtvochtigheid; frequenter en heviger wateroverlast in steden en landelijk gebied; frequenter en heviger grondwateroverlast; toenemende erosie en verslamping van de bodem.
3. **Het wordt droger:** toename droge lentes en zomers - gemiddelde neerslagtekort neemt toe; frequentere, langdurigere en intensere droogteperioden; grotere kans laagwater en droogvallen rivieren, beken, plassen, vennen, poelen in zomer; verslechtering oppervlaktewaterkwaliteit; lagere grondwaterstanden; versnelling bodemdaling;
4. **Overig extreem weer:** toename in frequentie en hevigheid van stormen, valwinden, tornado's, hagelbuien, onweer, bliksem, koudegolven, sneeuw en ijzel
5. **De zeespiegel stijgt:** hogere waterstanden aan de kust met risico op overstromingen vanuit zee; toenemende kweldruk landinwaarts; toenemende verzilting van grond- en oppervlaktewater; opstuwing en beperking afwatering.

4.2 Klimaatrisico's digitale infrastructuur

Bij de klimaatrisicoanalyse digitale infrastructuur is eerst een globale analyse uitgevoerd van de grootste risico's op basis van desk research, interviews met stakeholders en expert opinies. Bij de selectie van de grootste risico's is ook gekeken naar de huidige

adaptatiemaatregelen tegen het risico op verstoring in het algemeen en specifiek voor een klimaatrisico. Deze globale analyse is beschreven in deze paragraaf. Hierbij is gekeken naar de blootstelling van de generieke en sectorspecifieke digitale infrastructuur aan de verschillende klimaatdreigingen, waarbij de grootste risico's zijn geïdentificeerd voor nadere analyse in de contextscenario's. Voor de analyse naar de klimaatrisico's in de digitale infrastructuur is een aangepaste indeling gebruikt ten opzichte van de 5 componenten in de digitale infrastructuur (zie paragraaf 3.1). Dit is gedaan omdat klimaatrisico's specifiek effect hebben op de fysieke componenten van de digitale infrastructuur. In de analyse is de volgende indeling gebruikt om klimaatrisico per fysieke component in de digitale infrastructuur te kunnen bepalen.

- 1) **Fysieke datakabels** (glasvezel, koper en coax) in telecomnetwerken: in de vaste aansluitnetwerken voor breedband internettoegang, TV en vaste telefonie wordt gebruik gemaakt van verschillende aansluitnetwerken, met koper- en coaxkabels en in toenemende mate glasvezel. In het eerste kwartaal van 2025 was het aantal huishoudens met een glasvezelinternetabonnement 3,27 miljoen, met kabelabonnementen 3,16 miljoen, en de hoeveelheid koperabonnementen 1,97 miljoen [29]. Daarnaast worden er glasvezelkabels gebruikt in de vaste en mobiele netwerken voor dataverkeer tussen de verschillende fysieke locaties, zoals mobiele masten, straatkasten en regionale en landelijke locaties met technische apparatuur (servers, etc.) en naar internet (internet exchanges, datacenters, cloud). Daarnaast zijn er internationaal verbindingen via onderzeese datakabels en datakabels tussen landen.
- 2) **Fysieke masten en opstelpunten in mobiele telecomnetwerken**: masten en opstelpunten (op hoge gebouwen) worden gebruikt voor de mobiele netwerken, C2000 en voor radio- en TV. In de fysieke zendmasten worden antennes en actieve apparatuur geplaatst, in de mast of in een gebouw/kast onder aan de mast. Verder zijn er nog specifieke lokale netwerken voor bijv. maritieme communicatie en luchtvaartcommunicatie in aanvliegroutes en rondom vliegvelden.
- 3) **Fysieke locaties met netwerkapparatuur in vaste en mobiele telecomnetwerken**, zoals straatkasten/buitenkasten en andere gebouwen in het aansluitnetwerk en het datatransportnetwerk. Daarnaast hebben telecomnetwerken regionale en landelijke locaties met actieve apparatuur, die vergelijkbaar zijn met datacenters.
- 4) **Datacenters**, waaronder zowel internet exchanges als datacenters waarvan uit housing, hosting- of clouddiensten worden geboden. Datacenters zijn apart meegenomen door de specifieke klimaatrisico's die deels anders zijn dan voor de vaste locaties van telecomnetwerken en datacenters een andere functie hebben in de digitale infrastructuur (toegang tot informatie en applicaties).

4.2.1 Klimaatrisico's voor fysieke datakabels

De klimaatrisico's qua blootstelling en gevoeligheid voor datakabels zijn ingeschat op laag. De belangrijkste reden is dat de kabels ondergronds zijn, of op of net onder de zeebodem liggen in de Noordzee.

Datakabels zoals glasvezel zijn niet direct gevoelig voor droogte, aangezien deze zijn gemaakt van kunststof en glasvezel, en in bepaalde gevallen een mantel met metaal voor de sterkte. Deze materialen worden niet beïnvloed door vochtigheidsniveaus in de bodem. Ook worden glasvezels in buizen aangelegd om breuken bij verzakkingen of graafschade te beperken of te voorkomen. Wel kunnen kabels verschuiven, of verzakken ten gevolge van bodemdaling. De kans hierop neemt toe wanneer de grond gaat schuiven door afwisselend droogte en natheid. Bij graafwerkzaamheden is al vaker gebleken dat kabels een stuk verschoven waren, doordat de grond 'beweegt'. Bij (sterke) afwisseling van droogte en vocht kan er meer verschuiving plaatsvinden.

4.2.2 Klimaatrisico's voor masten en opstelpunten in mobiele netwerken

Voor masten en andere opstelpunten zijn drie klimaatdreigingen geïdentificeerd met een mogelijke verhoogd risico. De score van het risico's is 'midden' aangezien het optreden van een klimaatrisico zorgt voor lokale uitval van één of enkele masten, waarbij er een beperkt geografisch gebied wordt geraakt door verminderde of geen dekking bij verstoringen.

Hitte (oververhitting): de actieve apparatuur dat in een mast is gemonteerd kan gevoelig zijn voor verstoringen bij (langdurige) hitte en directe blootstelling aan zonlicht. Deze actieve apparatuur is ontworpen om te werken bij temperaturen tot 50°C. Deze apparatuur wordt steeds kleiner, waardoor deze meer en meer in masten wordt gemonteerd. Dit verhoogt het risico op directe blootstelling aan hitte en het risico van snellere veroudering door blootstelling. De actieve radioapparatuur (boven) in masten wordt meer blootgesteld aan hitte dan apparatuur in kasten (met koeling) onder bij een mast. Oververhitting kan schade brengen aan de apparatuur. Naar de toekomst toe worden er meer hitteperiodes verwacht. Volgens de Klimateffectatlas [30] zijn het aantal tropische dagen (>30°C) op dit moment gemiddeld 5 per jaar. In de klimaatscenario's zal dit toenemen naar 9-12 in 2050 en 9-30 in 2100.

Neerslag/overstroming: lokale overstromingen door extreme neerslag of door verhoogde afvoer in rivieren kan leiden tot wateroverlast in kasten/gebouwen bij masten, hetgeen weer kan leiden tot (structurele) instabiliteit. En mogelijk kan een overstroming ook de toegang blokkeren, waardoor er geen reparatie of vervanging van noodstroombatterij als deze leeg is, kan plaatsvinden. In het verleden heeft overstroming en stroomuitval ook geleid tot problemen in masten. Er was dan niet altijd noodstroom aanwezig, wat leidde tot een tijdelijke vermindering van de dekking van het mobiele netwerk.

Extreem weer (storm, extreme neerslag, wind, tornado's, hagel, sneeuw, ijzel, onweer, bliksem): Het extreme weer waar we in dit onderzoek naar kijken zijn sterke windstoten en storm, extreme neerslag en hagel. Extreem weer kan zorgen voor beschadiging van masten of actieve apparatuur in masten. Sterke windstoten en stormen kunnen masten beschadigen of zelfs omverwerpen, echter de mastconstructies zijn ontworpen en gebouwd tot windkracht 12. Masten zijn vaak een van de hoogste objecten in een gebied en kunnen daarom bliksem aantrekken. Wel zijn ze vaak uitgerust met bliksemafleiders om schade te voorkomen. Stormschade aan zendmasten is lokaal, wat maakt dat de impact minder groot is, al kunnen bij een orkaan of extreme windstoten, zoals die in het Caribische deel van Nederland kunnen voorkomen, wel meerdere masten in een gebied getroffen worden. Bij extreme neerslag kan

wateroverlast ontstaan in kasten of gebouwen direct onder of bij de zendmast, vooral als deze laaggelegen zijn. Zware hagelstenen kunnen mogelijk antennes en radioapparatuur in de masten beschadigen. Het gevolg van extreem weer is uitval van individuele masten, met lokale gevolgen voor radiodekking en capaciteit.

4.2.3 Klimaatrisico's voor vaste locaties met netwerkkapparatuur in telecomnetwerken

ICT-apparatuur bevindt zich in gebouwen, zoals datacenters of technische gebouwen van telecomaandieners, maar ook buiten in bijv. straatkasten. Zo lopen (glasvezel)kabels vaak niet van gebouw naar gebouw: zij gaan via 'knooppunten' (buitenkasten voor telecommunicatie) vanuit het aansluitnetwerk naar het regionale of landelijke data transportnetwerk) zoals straatkasten in wijken voor internet, telefonie en TV van consumenten of via kasten met optische versterkers voor verbindingen over grotere afstanden.

Hitte (oververhitting): Doordat kasten zich buiten bevinden en geen systemen voor klimaatbeheersing hebben wordt de IT-apparatuur in deze kasten meer blootgesteld aan temperatuurextremen en -wisselingen. Hogere temperaturen, zeker als deze frequenter optreden, vergroten de kans op uitval van de IT-systemen in buitenkasten en zorgen voor een kortere technische levensduur van de onderdelen.

Water (neerslag en waterpeilstijging en overstromingen door extreme neerslag): Voor telecomkasten voor het vaste of mobiele netwerk, liggend op maaiveld, wordt uitval bij 20 cm waterdiepte genoemd [31]. De kritische uitvalhoogte in [32] noemt 20-30 cm voor straatkasten voor elektriciteit, 40-50 cm voor telecomwijkkasten, 20-30 cm voor besturingskasten in afvalwaterinstallaties, 10-30 cm voor verschillende schakelkasten bij rioolzuivering en 0-20 cm voor schakelkasten in poldergemalen. Overschrijding van deze waarden zorgt doorgaans voor uitval van functie, bijvoorbeeld uitval van het poldergemaal. Het is wisselend per type kast of er redundantie is. Straatkasten zijn meestal niet volledig waterdicht tegen hoog water bij overstroming [33]. Straatkasten zijn ook niet of beperkt redundant uitgevoerd, met een beperkt aantal getroffen gebruikers per straatkast.

Extreem weer (storm, extreme neerslag, wind, tornado's, hagel, sneeuw, ijzel, onweer, bliksem): Door meer extreem weer is er enigszins meer kans op uitval door beschadiging, voornamelijk door water en extreme wind (direct door bijvoorbeeld blikseminslag of indirect door bijvoorbeeld omvallende bomen). Over het algemeen is de impact vrij lokaal.

Droogte (Schaarste koelwater, bodemdaling): Meer droogte heeft geen directe gevolgen op straatkasten of andere vaste locaties met netwerkkapparatuur in telecomnetwerken.

4.2.4 Klimaatrisico's voor datacenters

Datacenters zijn in te delen in drie types, zoals te zien in Figuur 6:

- Single tenant private/enterprise: dit zijn datacenters van één bedrijf of organisatie die enkel worden gebruikt voor eigen servers van een organisatie. De datacenters van Defensie zijn hier een voorbeeld van, deze worden alleen gebruikt door het Ministerie van Defensie;

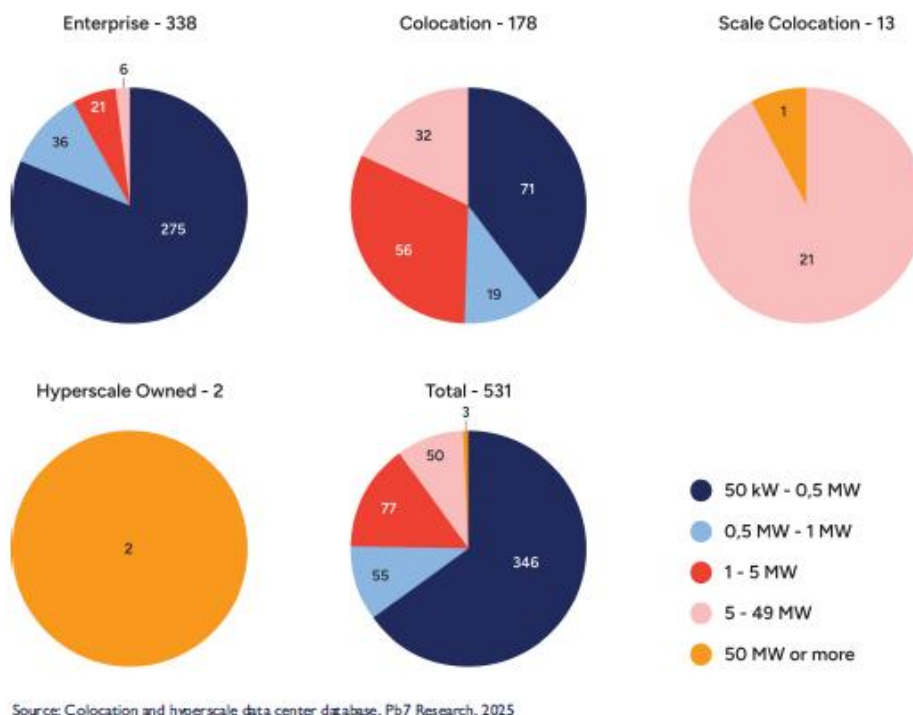
- Colocatie (regionaal, nationaal, internationaal): dit zijn datacenters die worden gebruikt voor housing en hosting diensten aan meerdere bedrijven of organisaties. Afhankelijk van datacenter wordt het gebruikt voor regionale, nationale of internationale colocatie diensten. Ook bedrijven zoals Amazon, Google en Microsoft maken, naast hun eigen hyperscale locaties, gebruik van colocatie datacenters als zogeheten satellietlocaties in de buurt van een eigen hyperscale datacenter, ter uitbreiding op capaciteit;
- Single tenant hyperscale: dit zijn de grote datacenters van bedrijven als Amazon, Google en Microsoft voor hun clouddiensten.

The different types of data centers are typically categorized as follows:

	SINGLE TENANT	COLOCATION DATA CENTER			SINGLE TENANT
Type	PRIVATE/ENTERPRISE including server spaces	REGIONAL	NATIONAL	INTERNATIONAL	HYPERSCALE
Customers	SME Enterprise Public Semi-public	SME Public Semi-public	SME Enterprise Cloud Public Semi-public	SME Enterprise Cloud SaaS	Cloud SaaS
Space Impact	> 10 m2 Small	> 200 m2 Small	> 2000 m2 Small	> 5000 m2 Medium	> 5 ha Medium/Large
Energy Impact	0,01 - 10 MW Small	0,5 - 10 MW Small	1 - 10 MW Medium	> 5 MW Medium	> 50 MW Large
Location (approximity)	In every province	In every province	In (regional) hubs	Amsterdam hub	Outskirts

Figuur 6 Verschillende types datacenters en kenmerken. Bron: Dutch Data Center Association (2024)

Als men enkel kijkt naar type en aansluitcapaciteit voor elektriciteit (IT vermogen) dan komt men in Nederland tot onderstaande verdeling in aantallen, met enterprise en colocatie vanaf 50 kW+, scale colocatie typisch tussen 20-80 MW en hyperscale vanaf 70 MW. In aantal is het type enterprise dominant (338 van 531, 64%), in IT vermogen is colocatie (62%) dominant, gevolgd door hyperscale (30%) en enterprise (8%).



Figuur 7 Datacenters in Nederland per type en IT vermogen (50kW or more), 2024EY [Bron: State of the Dutch Data Center 2025, DDCA, [State of the Dutch Data Centers 2025 - Dutch Data Center Association](#)]

Datacenters hanteren doorgaans hoge beschikbaarheidseisen, waardoor veel redundantie is ingebouwd, zowel op gebied van fysieke aansluitingen voor elektriciteitsvoorziening (twee gescheiden aansluitingen via de netbeheerder) en fysieke datakabels als het gebruik van meerdere (back-up) locaties. Dit laatste is ook voor klimaatadaptatie bruikbaar: zo kunnen 'tweeling' locaties (een tweede identieke locatie waarop kan worden overgeschakeld bij uitval, datacenter *twinning*) worden gekozen die bijv. niet in hetzelfde overstroomingsgebied liggen en niet op dezelfde regionale netbeheerder of op hetzelfde middenstation van een netbeheerder zijn aangesloten voor elektriciteit, etc. [interview Bytesnet]. Als grootverbruikers van (duurzame) elektriciteit hebben zij steeds meer moeite met het vinden van geschikte locaties en wordt er geanticipeerd om meer elektriciteitsstoringen [34]. Back-up systemen voor noodstroom (aggregaten, vaak op basis van diesel) zijn daardoor veel voorkomend, vaak met grote brandstofvoorraden (genoeg voor meerdere dagen tot een week) [interview TNO, expert robuustheid kritieke ICT systemen, interview Bytesnet].

Hitte (oververhitting): Hitte veroorzaakt een hogere elektriciteitsvraag voor de koeling bij datacenters (koeling is zo'n 10-30% van het energieverbruik van een datacenter [34]), en bij temperaturen boven de 25°C stijgt ook de watervraag (zie droogte voor verdere uitwerking). Bij onvoldoende koelcapaciteit moet hardware worden afgeschakeld (automatisch), wat leidt tot uitval van functionaliteit, maar er ontstaat doorgaans geen permanente hardware schade [Interview Bytesnet]. ICT-hardware zoals servers, routers en dataopslag is uitgerust met temperatuurmeters (o.a. om ingebouwde ventilator in en uit te schakelen). Echter, die temperatuurmeter wordt tegenwoordig ook gebruikt om *graceful shutdown* te doen als een bepaalde (instelbare) drempelwaarde wordt overschreden, en deze ligt veel lager dan de temperatuur waarbij defecten optreden (boven 35°C graden gaat apparatuur al minder goed

werken en per graad stijging heeft het dus minder zin om het apparaat aan te laten staan). Om dat te voorkomen zijn er richtlijnen die voorschrijven dat aanvullende koeling al rond 27°C moet worden aangezet. Als preventieve maatregel liggen dergelijke drempelwaarden dus een heel stuk lager dan temperaturen (typisch tot 50°C) waarbij hardware defect raakt. Bij gebruik van twee of meerdere (back-up) locaties zorgt de afschakeling van (apparatuur op) één locatie ook niet tot verstoring van de ICT-diensten.

Water (neerslag en waterpeilstijging en overstromingen door extreme neerslag): Extreme regenval en een stijgende zeespiegel vormen een bedreiging voor datacenters, direct door mogelijke waterschade van installaties en/of ICT-apparatuur, indirect door uitval/afschakeling van elektriciteit in overstroomde gebieden. Veel datacenters zijn gelegen in lage gebieden: 23 van de 56 datacenterhubs staat bijvoorbeeld in de regio Amsterdam [34], waarvan veel in de Haarlemmermeer, een laag gebied¹. Klanten (zeker Amerikaanse) vragen vaak om bouwhoogte van +1 m NAP [interview Bytesnet], maar dat is niet altijd mogelijk. Het plaatsen van alle technische systemen naar hogere verdiepingen is maar deels mogelijk: apparatuur zoals transformatoren moet van buiten direct toegankelijk zijn voor netbeheerders en brandweer [interview Bytesnet], waardoor overstroming toch in de meeste gevallen tot uitval leidt.

Extreem weer (storm, extreme neerslag, wind, tornado's, hagel, sneeuw, ijzel, onweer, bliksem): Extreem weer heeft relatief weinig effect op datacenters, buiten de overstromingsrisico's, vanwege strenge bouweisen.

Droogte (schaarste koelwater, bodemdaling): De meeste datacenters maken gebruik van luchtkoeling, met waterkoeling voornamelijk ingezet op warmere dagen boven 25°C [35]. Er zijn gesloten en open waterkoeling systemen mogelijk (dit is een keuze bij datacenter ontwerp), open systemen gebruiken hoge volumes water op piekmomenten (bij warm weer). Het klimaatrisico langdurige droogte in combinatie met hitte is een indirect risico in dien er restricties op drinkwater of oppervlaktewater voor koeling van datacenters worden opgelegd door de overheid. Daarnaast is er een indirect risico dat gebruikt koelwater niet geloosd mag worden als de temperatuur van het oppervlaktewater en/of het gebruikt koelwater te hoog is.

De gevolgen van een gebrek aan koelwater is uitschakeling van (een deel van) de servers in het datacenter. Veel datacenters hebben als back-up een eigen watervoorraad, met contracten voor bijvullen [interview Bytesnet].

Zeespiegelstijging: Zeespiegelstijging verhoogt voornamelijk het overstromingsrisico in de context van datacenters. Zout water kan wel meer corrosieve effecten hebben, maar meestal maakt de watersoort niet uit: als hardware in een datacenter onder water komt te staan is het kapot [interview Bytesnet].

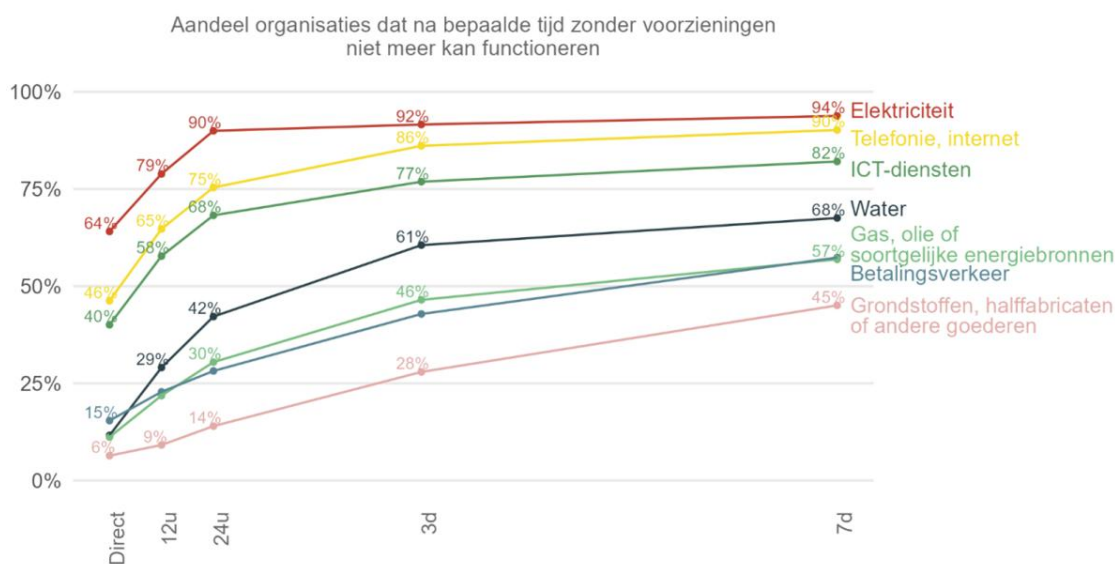
4.2.5 Indirect klimaatrisico door (grootschalige) uitval van stroomvoorziening

Het grootste klimaatrisico voor de digitale infrastructuur is een **secundair effect** dat optreedt bij **(grootschalige) uitval van stroomvoorziening** door het optreden van klimaatrisico's.

¹ Risicokaart overstromingen: <https://www.risicokaart.nl/kaarten/risicosituaties/overstroming> en de hoogtekkaart Nederland: <https://www.ahn.nl/ahn-viewer>

Voor (hyperscale) datacenters en centrale netwerklocaties worden back-up voorzieningen (UPS) gebruikt die meerdere dagen kunnen blijven werken. Echter, richting de 'randen' van de netwerken en voor de internet en netwerkaansluitingen voor bedrijven en consumenten is er geen back-up of zeer beperkte back-up van 2-3 uur (bijv. in mobiele masten) vanuit het netwerk. Hierdoor zal een groot deel van de bedrijven en consumenten geen gebruik meer kunnen maken van ICT en internet, tenzij men zelf lokale back-up voorzieningen heeft.

In hoofdstuk 7 is gekeken naar een studie naar cascade- en keteneffecten die optreden bij uitval van stroomvoorziening en ICT, en het effect op andere sectoren, zoals OOV. In onderstaande figuur is weergegeven welk deel van de organisaties niet meer kan functioneren zonder essentiële voorzieningen: direct, na 12 uur, na 24 uur, na 3 dagen en na 7 dagen. Na 24 uur kan bijv. het grootste deel van de organisaties niet meer functioneren: 90% bij uitval van elektriciteit, 75% bij uitval van telefonie en internet en 68% bij uitval van ICT-diensten. van de organisaties. Dit toont de grote afhankelijkheid van elektriciteit en ICT, en de noodzaak tot maatregelen bij uitval , ook voor klimaatrisico's.



Bron: De Nederlandse Innovatie Monitor 2025, bewerking door SEO Economisch Onderzoek

Noot: Gebaseerd op 311 waarnemingen, gewogen naar representativiteit voor de Nederlandse bedrijvenpopulatie exclusief zzp'ers (zie Bijlage A.2).

Figuur 8 Kwetsbaarheid Nederlandse bedrijfsleven voor uitval van essentiële voorzieningen (Bron: SEO [36])

Verder laat een recente studie van SEO [36] de kwetsbaarheid zien van het Nederlandse bedrijfsleven voor uitval van essentiële voorzieningen, zoals elektriciteit, telefonie en internet, ICT-diensten en water.

4.3 Selectie van klimaatrisico's

Er is een globale beoordeling gemaakt van de belangrijkste klimaatrisico's voor de digitale infrastructuur op basis van expert opinies, zie Tabel 1. Voor de inschatting is gekeken naar de omvang van een klimaatrisico op basis van de huidige digitale infrastructuur en de urgentie voor adaptatie voor klimaatdreigingen **tot 2050**. Door de snelle technologische ontwikkelingen binnen de digitale infrastructuur is het voor de periode 2050-2100

onvoldoende duidelijk hoe de fysieke, digitale infrastructuur zich ontwikkelt, binnen Nederland en binnen Europa en wat het effect is op klimaatrisico's. Sinds de komst van internet en de introductie van steeds snellere vaste (glasvezel) en mobiele netwerken (nu 5G, satelliet) is de digitale infrastructuur sterk verandert, zowel in technologie (bijv. van telefonie naar data), gebruik (browsen, social media, AI) als de marktspelers (van nationaal naar BigTech). Toekomstige infrastructuur zal beter voorbereid zijn op (klimaat)risico's, en de cyclus van vernieuwingen is typisch 5 tot 10 jaar voor actieve apparatuur. Voor de fysieke gebouwen zelf en de fysieke (glasvezel)verbindingen is dit typisch 10-20 jaar.

De globale beoordeling is gebruikt als eerste stap om vervolgens een meer gedetailleerde analyse uit te voeren naar de werkelijke omvang van de klimaatrisico's, aangezien het niet noodzakelijk is om ook minimale klimaatrisico's in detail te analyseren. In Tabel 1 is het overzicht gegeven met de globale inschatting van de klimaatrisico's (laag/midden/hoog) voor de vier componenten in de digitale infrastructuur (zie sectie 4.2) en de vijf klimaatdreigingen (zie sectie 4. De geselecteerde klimaatrisico's hebben het label 'midden' of 'midden/hoog', zoals aangegeven in Tabel 1.

Tabel 1 Klimaatrisico (laag/midden/hoog) voor i) de huidige digitale infrastructuur met vier elementen en ii) de vijf klimaatdreigingen. De geselecteerde klimaatrisico's (midden en midden/hoog) voor verdere analyse in hoofdstuk 4 zijn in het oranje aangegeven

	Hitte	Lokale wateroverlast	Extreem weer	Droogte	Zeespiegelstijging
Datakabels	Laag	Laag	Laag	Laag	Laag
Masten	Midden	Midden	Midden	Laag	Laag
Vaste locaties	Laag	Midden	Laag	Laag	Laag
Datacenters	Midden/Hoog	Midden	Laag	Midden/Hoog	Midden

De klimaatrisico's van hitte en langdurige droogte zijn samen genomen doordat ze elkaar versterken namelijk het effect van langdurige droogte op watertekorten voor koeling in datacenters op zomerse en tropische dagen.

Datakabels

Hitte, extreem weer en lokale wateroverlast vormen geen risico voor de ondergrondse datakabels. Vanuit de desk research en de interviews met stakeholders uit de telecomsector zijn er ook geen signalen ontvangen dat bodemdaling leidt tot een hoger risico op breuken in glasvezelkabels. Het grootste risico op kabelbreuk is door graafschade bij bouwwerkzaamheden. Om deze redenen is er geen nadere analyse gedaan naar het klimaatrisico's op fysieke ondergrondse datakabels in de contextscenario's voor 2050 en 2100.

Masten en opstelpunten

Hitte, extreem weer en lokale wateroverlast vormen mogelijk een risico voor mobiele masten en opstelpunten, aangezien actieve apparatuur in buitenkasten bij een mast of in de mast zijn geïnstalleerd. In de analyse zijn deze meegenomen in:

- ☐ Masten en hitte: schade aan elementen in masten door oververhitting;
- ☐ Masten en extreem weer met lokale wateroverlast: schade aan masten door storm, bliksem en wind of lokale wateroverlast door extreme buien of overstroming vanuit rivieren.

Vaste locaties

De klimaatrisico's voor buitenkasten in vaste netwerken zijn vergelijkbaar met de buitenkasten bij mobiele masten en zijn niet apart meegenomen. Deze buitenkasten beschikken niet over klimaatbeheersing (koeling, ventilatie etc.) Het risico op lokale wateroverlast bij buitenkasten is onderdeel van bovenstaande analyse naar masten en extreem weer. De grotere locaties in telecomnetwerken beschikken veelal wel over klimaatbeheersing bij hitte en zijn veelal voldoende bestand tegen wateroverlast o.a. doordat er gebruik wordt gemaakt van verhoogde vloeren, ICT-apparatuur die op hoogte geplaatst wordt in kasten of, indien mogelijk, op een hogere verdieping.

De hoofdlocaties in de telecomnetwerken van KPN, Odido en VodafoneZiggo zijn vergelijkbaar met single-tenant datacenters, d.w.z. specifieke locaties van een telecom operator met klimaatbeheersing etc. Er is daarom geen aparte analyse gedaan naar de klimaatrisico's voor deze hoofdlocaties.

Datacenters

Het klimaatrisico van langdurige droogte in combinatie met hitte vormt een indirect risico. Dit risico treedt op indien er restricties op gebruik van drinkwater of oppervlaktewater voor koeling van datacenters worden opgelegd door de overheid, waardoor datacenters gedwongen worden om (een deel van de) apparatuur uit te zetten. Daarnaast is er een indirect risico dat gebruikt koelwater niet geloosd mag worden als de temperatuur van het oppervlaktewater te hoog is.

79% van de datacenters gebruikt drinkwater voor koeling, 21% gebruikt water die zij zelf filteren (en dit percentage stijgt) [34], uit regenwater of oppervlaktewater. De sector ICT als geheel gebruikt jaarlijks minder dan 0,1%² van het drinkwater [37], maar op lokaal niveau is dit percentage hoger en het watergebruik is vooral hoog tijdens hete (en dus wellicht droge) periodes. In de Verdringingsreeks bij watertekort (Besluit kwaliteit leefomgeving Artikel 3.14) valt water voor datacenterkoeling namelijk in de laatste categorie, wat betekent dat zij geen prioriteit krijgen bij watertekort. Adaptatiemogelijkheden zijn het gebruik van, in plaats van drinkwater, oppervlaktewater, industrieel water, of regenwater vanuit opslag [interview Dialogic] en het kiezen van locaties met kleine kans op watertekorten. Bovendien zijn ook gesloten systemen mogelijk (maar deze zijn wel minder efficiënt), hierbij is geen (extra) water nodig. Ook zijn andere koelingsoplossingen in opkomst (zoals gesloten systemen met vloeistof), dit is vooral efficiënt voor rekenintensieve modules (GPU) die veel gebruikt voor AI-berekeningen). Ook is een combinatie met het gebruik van restwarmte uit datacenters voor stadsverwarming of industriële processen mogelijk [interview Dialogic en Bytesnet].

Verder vormt uitval of afschakeling van een datacenter bij lokale wateroverlast een reëel risico en is dit risico ook geselecteerd. In de analyse zijn daarom de volgende twee klimaatrisico's voor datacenters meegenomen:

- ☐ Datacenters en hitte/droogte: datacenters moeten afschakelen door koelingsproblemen;
- ☐ Datacenters en overstroming: schade aan datacenters door overstroming door lokale wateroverlast (bij extreme neerslag) en zeespiegelstijging.

Selectie klimaatrisico's voor de verschillende contextscenario's

De geselecteerde klimaatrisico's voor nadere analyse in hoofdstuk 4 en 5 zijn:

1. Masten en hitte: schade aan elementen in masten door oververhitting;

² 1,0 mln m³ op 1125,3 mln m³ drinkwater in 2021

2. Masten en extreem weer en lokale wateroverlast: schade aan masten door storm, bliksem en wind;
3. Datacenters en hitte/droogte: datacenters moeten afschakelen door koelingsproblemen of doordat gebruikt koelwater niet geloosd kan worden op oppervlaktewater;
4. Datacenters en overstroming: schade aan datacenters door overstroming door lokale wateroverlast (bij extreme neerslag) en zeespiegelstijging.

Voor de klimaatdreiging droogte is er het directe risico voor de digitale infrastructuur laag, er is enkel een indirect risico voor datacenters in combinatie met hitte, zie hieronder.

Door bodemdaling is er wel kans op verzakking van de fundering van masten of gebouwen. De waarschijnlijkheid en impact hiervan is niet meegenomen, dit is onderdeel voor de analyse binnen de sector Gebouwde Omgeving. Binnen de telecomsector wordt verzakking van funderingen van masten door bodemdaling momenteel niet gezien als reëel klimaatrisico.

Er is wel een indirect risico bij droogte. Een regionaal watertekort bij droogte in combinatie met een periode van extreme hitte kan leiden tot beperkende maatregelen in laagwaardig (drink)watergebruik. Dit zal datacenters raken, die drinkwater gebruiken voor koeling en klimaatbeheersing (luchtvochtigheid) in deze gebouwen.

Voor zeespiegelstijging geldt het risico op grootschalige overstroming door hogere waterstanden. Ook een lokale (door wateroverlast bij extreme buien) of grootschalige overstroming (door wateroverlast door rivieren) heeft direct gevolgen voor de digitale infrastructuur, aangezien elektriciteit en ICT zal uitvallen en daarnaast kunnen gebouwen en de actieve apparatuur in deze gebouwen beschadigd raken. In de analyse zijn de risico's voor overstromingen door lokale wateroverlast of zeespiegelstijging samen genomen.

5 Klimatrisicoanalyse digitale infrastructuur bij huidig beleid

Er zijn verschillende risico's die leiden tot uitval van fysieke componenten in de digitale infrastructuur. Denk aan uitval van de stroomvoorziening of koelsystemen van datacenters, uitval van een netwerkelement (switch, router) of server, of een kabelbreuk in glasvezels door graafwerkzaamheden. Daarnaast spelen cyberdreigingen een steeds grotere rol en ook worden veel verstoringen nog steeds veroorzaakt door menselijk handelen, bijv. bij een software-update. Deze risico's zijn veelal groter dan de klimatrisico's, met name door de grotere kans op het optreden van het specifieke risico, zie bijv. voor datacenters in [38].

Aanbieders van telecom- en datacenter/clouddiensten maken gebruik van risicomanagement om alle risico's te identificeren, maatregelen te definiëren en in te voeren en risico's te monitoren, veelal vanuit financieel oogpunt. Klimatrisico's hebben hierin de laatste jaren een grotere aandacht gekregen door de klimaatverandering en het belang van duurzaamheid en het verminderen van de ecologische voetafdruk van de digitale sector. Hierbij wordt door een groot deel van de vitale aanbieders van digitale infrastructuur de methodiek gebruikt die is ontwikkeld vanuit de *Task force on Climate-related Financial Disclosures*, TCFD [39]. Dit werk is sinds oktober 2023 overgenomen door IFRS foundation [40]. De methodiek kent vier pijlers: besturing (governance), strategie, risico management en statistieken en doelstellingen. Klimatrisico's worden meegenomen in het bestaande risicomanagement en worden waar mogelijk financieel gemaakt. De directe kosten bij een ernstige verstoring van meerdere uren kan bij een telecom- of datacenteraanbieder oplopen tot meer dan 1 miljoen EUR, naast de imagoschade. Daarnaast wordt ook gekeken naar mogelijkheden (*opportunities*), zoals overstap naar schone energie, besparing op energieverbruik, weerbaarheid met meer aandacht voor diensten met hogere redundantie, en diensten die beter scoren op duurzaamheid t.o.v. concurrenten.

Binnen de methodiek van TCFD wordt onderscheid gemaakt in fysieke klimatrisico's, met onderscheid in acuut (extreem weer, overstroming, etc.) en chronisch (langdurige hittegolven, droogte, zeespiegelstijging), en in risico's ten gevolge van de transitie naar klimaatneutraal (policy en wetgeving, technologie, markt, reputatie). Door het toepassen van deze methodiek worden klimatrisico's continue in kaart gebracht en worden - op basis van feitelijke informatie (incidenten en statistiek) maatregelen genomen, en vindt continue adaptatie plaats op basis van veranderingen in risico's en verandering van ICT-infrastructuur.

5.1 Huidige beleid en wetgeving

Voor de telecomsector gelden indirecte kaders vanuit de Telecomwet en voor vitale entiteiten de Wwke en de Cbw. De drie mobiele operators in Nederland geldt de Telecomwet en zij zijn ook aangewezen als aanbieders van vitale infrastructuur, met bijbehorende verplichting rondom continuïteit (Telecomwet, hoofdstuk 11a en specifiek artikel 11a.3 voor antenne-opstelpunten) en de Wwke en Cbw. Hierbij zijn geen specifieke verplichtingen opgenomen

ten aanzien van maatregelen tegen de verschillende klimaatrisico's in telecomnetwerken (masten, buitenkasten, regionale en centrale netwerklocaties), enkel ten aanzien van de zorgplicht die is gericht op continue of maximale beschikbaarheid.

Specifiek voor datacenters gelden zowel directe als indirecte kaders op het gebied van duurzaamheid en energie, die kunnen variëren van regionaal, nationaal tot Europees niveau. In de Kamerbrief [41] van de Minister van EZ (DGED/89399224, 21 nov. 2024) over datacenters in de Nederlandse digitale economie is het huidige beleid toegelicht. Hieronder is globaal het huidige beleid ten aanzien van datacenters beschreven vanuit vier punten:

- ☐ economisch,
- ☐ ruimtelijke inrichting,
- ☐ duurzaamheid en
- ☐ vitale infrastructuur.

In de praktijk zal er altijd een afweging gemaakt worden moeten worden tussen de verschillende keuzes, zowel binnen de digitale sector verantwoordelijk voor de digitale infrastructuur, als tussen sectoren. Ook kan beleid en wetgeving rondom de digitale infrastructuur in Nederland niet los worden gezien van Europese ontwikkelingen.

1. Economisch beleid

Datacenters zijn een belangrijk onderdeel van de digitale infrastructuur en daarmee van groot belang voor het innovatie- en verdienvermogen van Nederland. Tevens hebben zij een rol bij de borging van de (digitale) open strategische autonomie. Nederland heeft een belangrijk internet-knooppunt (AMS-IX) in de Metropoolregio Amsterdam of MRA, dat onderdeel is van het netwerk tussen belangrijke internetknooppunten (Frankfurt, Londen, Amsterdam, Parijs en Dublin, FLAPD) in Noordwest Europa. In deze regio's zijn veel datacenters gevestigd met hyperconnectiviteit. Nederland wil deze positie behouden, door ruimte te bieden voor (uitbreidingen) van hyperscale datacenters en (zee)datakabels naar andere delen van Europa. De MRA omvat ruwweg alle faciliteiten binnen een straal van 25 kilometer van het Amsterdam Science Park: Amsterdam zelf, Haarlemmermeer, Schiphol en zo'n 15 tot 20 omliggende gemeenten zoals Almere, Haarlem en Hilversum. Dit gebied is goed voor ongeveer 73% (eind 2024) van de landelijke colocatiecapaciteit (op basis van IT vermogen) [42]. Andere regio's met kleinere clusters van datacenters zijn Middenmeer in Noord-Holland, Groningen, regio Eindhoven (Hightech campus) en Rotterdam (havengebied).

2. Ruimtelijk beleid

Vanuit het kabinet bestaat geen stimuleringsbeleid voor de vestiging van datacenters. Er gelden wel restricties voor toewijzing van nieuwe locaties voor grote hyperscale datacenters (>10 ha en/of >70 MW aansluitvermogen). Alleen de Rijksoverheid kan nieuwe locaties aanwijzen, lokale overheden niet. Initiatieven voor groei of nieuwvestiging van datacenters, of clustering daarvan in bijvoorbeeld de vorm van Tech-campusen, moeten uit de regio of de sector komen. De rol van het Ministerie van EZ is faciliterend (werkgroep). Beleidsvorming over de ontwikkeling van datacenters of clusters daarvan, is gekoppeld aan het traject van de Ruimtelijke Economische Visie. Daarmee wordt dit integraal meegewogen in de door het kabinet te maken ruimtelijke keuzes bij de totstandkoming van de Nota Ruimte, onder regie van de Minister van Volkshuisvesting en Ruimtelijke Ordening.

Nederland kent momenteel alleen restricties voor hyperscale datacenters en de Rijksoverheid heeft momenteel twee locaties aangewezen voor hyperscale datacenters (Agriport A7 in Middenmeer, Noord-Holland en Dataport Eemshaven in Groningen) met een

verbod op uitbreiding op andere locaties. Naast de Rijksoverheid hebben de gemeenten Amsterdam en Haarlemmermeer, de MRA en de provincie Noord-Holland beleid t.a.v. nieuwe datacenters en uitbreidingen, gelet op ruimtelijke inpassing, energie- en watergebruik en restwarmte.

3. Beleid duurzaamheid, duurzame digitalisering

Alle economische activiteiten in Nederland zijn onderworpen aan regelgeving. Dat geldt ook voor datacenters. Bestaande generieke kaders en normeringsopties voor ruimtelijke ordening en impact op het milieu, en bestaande randvoorwaarden en standaarden met betrekking tot datacenters, bieden voldoende mogelijkheden om deze sector te reguleren. Een overzicht van deze directe en indirecte kaders is beschreven in de bijlage [43] bij de Kamerbrief.

In de Strategie Digitale Economie (Kamerstuk 26643 nr. 941) en, uitvoeriger, in de Staat van de Digitale Infrastructuur (Kamerstuk 26643 nr. 1119) is ingegaan op het belang van de digitale infrastructuur en is tevens de ecologische footprint daarvan in kaart gebracht. Met het Actieplan Duurzame Digitalisering (Kamerstuk 26643, nr. 1196) is de ambitie benadrukt om digitalisering en verdere verduurzaming hand in hand te laten gaan. Dit brengt dilemma's met zich mee tussen enerzijds de kansen voor innovatie, groei en het creëren van maatschappelijke meerwaarde door digitalisering en anderzijds de beperkingen en negatieve effecten daarvan. De belasting van het elektriciteitsnetwerk, het gebruik van drink- of zoetwater voor koelingsdoeleinden en in mindere mate het ruimtebeslag, stellen beperkingen aan de groei van datacenters.

Op basis van deze wetgeving is er ook binnen de digitale sector al veel aandacht voor de ecologische footprint, en specifiek voor datacenters door groei in stroomverbruik, onder andere veroorzaakt door groei van clouddiensten en high-performance computing toepassingen zoals AI en crypto (mining). Dit dwingt de sector om maatregelen te nemen om het energie- en waterverbruik te verminderen en de CO₂-uitstoot te reduceren tot nul in 2050. De sector zelf streeft naar nul uitstoot in 2030.

Het voordeel van de digitale sector is dat het bijna 100% gebruik maakt van elektriciteit als energiebron, niet van fossiele brandstoffen, en dat men daarmee gebruik kan maken van duurzame bronnen. Uitzonderingen zijn noodstroomvoorzieningen (back-up) die op fossiele brandstoffen werken (dieselgeneratoren), die slechts beperkt worden gebruikt, periodiek bij het testen van de juiste werking van de noodstroomvoorziening en incidenteel bij een stroomstoring. Er zijn ook voorbeelden van noodstroomvoorzieningen met brandstofcellen op waterstof. Het energieverbruik van de digitale sector zal in de komende jaren wel (sterk) blijven groeien, ondanks maatregelen voor efficiënter energiegebruik.

4. Beleid rondom vitale infrastructuur

Om de weerbaarheid van Europese lidstaten te versterken heeft de Europese Unie eind 2022 de Critical Entities Resilience Directive (CER-richtlijn, EU2022/2557) aangenomen [44]. Het doel daarvan is om de vitale infrastructuur en economische activiteiten in Europa zo goed mogelijk te beschermen tegen allerlei soorten dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen. Daarnaast is door de EU de Network and Information Security Directive (NIS2-richtlijn, EU2022/2555) aangenomen om de cyberbeveiliging te verhogen. Deze richtlijnen zijn gericht op een versterking van de fysieke, digitale en economische weerbaarheid van Europese lidstaten. Sinds januari 2023 werkt de Rijksoverheid aan de nationale implementatie door de richtlijnen om te zetten naar Nederlandse wetgeving. De NIS2-richtlijn wordt geïmplementeerd in de Cyberbeveiligingswet

(Cbw) en de CER-richtlijn in de Wet weerbaarheid kritieke entiteiten (Wwke). In de Wwke en de Cbw zijn meerdere entiteiten opgenomen, waaronder aanbieders van datacenterdiensten, cloudcomputing en openbare elektronische communicatienetwerken (zie paragraaf 3.3, trend 2).

In de wetsvoorstellen voor de Wwke en de Cbw zijn klimaatrisico's niet expliciet beschreven, anders dan natuurrampen, maar deze zijn wel impliciet beschreven, "alle relevante natuurlijke en door de mens veroorzaakte risico's die tot een incident zouden kunnen leiden". Hiermee kan de Wwke en de Cbw worden gebruikt om ook klimaatrisico's bij kritieke en/of essentiële entiteiten mee te nemen bij de risicobeoordeling door overheid en sectoren en te nemen maatregelen. De Cbw is ook van toepassing op kritieke entiteiten uit de Wwke, d.w.z. dat bijv. partijen uit energie of transport sector ook een zorgplicht hebben voor hun netwerk- en informatiesysteem.

Deze wetgeving is dus gericht op aanvullende maatregelen voor vitale aanbieders in zowel de digitale infrastructuur als in andere sectoren. Voor de digitale infrastructuur richt de Wwke en Cbw zich op de grotere aanbieders in vitale delen van de digitale infrastructuur. Deze worden door de overheid aangewezen op basis van omvang bijv. aantal klanten, aansluitvermogen datacenter, etc. Deze vitale aanbieders zijn belangrijk vanuit economisch perspectief, verstoring van diensten heeft een groot effect op de maatschappij.

Binnen de Wwke zijn verplichtingen opgenomen rondom risicobeoordeling, zorgplicht en meldplicht. Kritieke entiteiten moeten een eigen risicobeoordeling uitvoeren ten aanzien van alle relevante dreigingen die hun dienstverlening kunnen verstoren. Het doel is om potentiële dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden, in kaart te brengen en om in te schatten hoe groot de impact van een incident is op de essentiële dienstverlening. Hieronder vallen dreigingen ten gevolge van sectoroverstijgende of grensoverschrijdende aard en natuurrampen. De Wwke wordt indirect een instrument om informatie over de risicobeoordeling voor natuurrampen te krijgen. Verstoringen door klimaatrisico's zullen hierin opgenomen moeten worden, bijv. voor overstromingen en grootschalige stroomuitval. Maatregelen tegen (klimaat)risico's zullen primair bij de organisaties zelf liggen. Mogelijk is vanuit de overheid aanvullend beleid nodig om de gevolgen van stroomonderbrekingen op de digitale sector te beperken: hierbij kan men denken aan voorrang bij herstel van de stroomvoorziening, 'eigen' aansluitingen voor hyperscale datacenters, via meerdere aanbieders, en minimale voorzieningen voor gedeelde back-up (noodstroom, eventueel via waterstof) op datacenter hub-locaties.

5.2 Masten en hitte

5.2.1 Klimaatdreiging(en)

In paragraaf 4.2 zijn de klimaatrisico's voor de verschillende onderdelen binnen de digitale infrastructuur beschreven.

Er is in de nadere risicoanalyse geen onderscheid gemaakt tussen het contextscenario 'beperkt risicoverhogend' en 'sterk risicoverhogend', aangezien er beperkte kwantitatieve informatie beschikbaar is over het risico. Kwalitatief kan worden genoemd dat de kans op oververhitting toeneemt als er meer extreem warme dagen zijn. Er is een specifieke studie

naar uitval van radio transceivers in een kritisch privaat netwerk, waaruit bleek dat uitval van transceiver apparatuur veel sterker afhankelijk was van temperatuur en schommeling gedurende dag/nacht, dan van veroudering of onderhoudswerkzaamheden. Nieuwe apparatuur zal naar verwachting beter bestand is tegen hitte en temperatuurswisselingen o.a. door kleinere apparatuur en computerchips. Verder zijn er geen secundaire effecten bekend van hitte op masten.

5.2.2 Adaptatiemaatregelen huidig beleid

Adaptatiecapaciteit vanuit de sector

Mobiele netwerken bestaan uit een groot aantal masten (ca. 16.000, november 2025 [45]) en er zijn drie mobiele netwerken in Nederland met vergelijkbare dekking. Incidentele uitval van een mast door extreem weer in één van de drie mobiele netwerken blijft beperkt tot een lokaal effect: verminderde dekking voor abonnees van de getroffen mobiele netwerk operator (MNO), totdat dit hersteld is. Herstel vindt typisch plaats binnen 4 tot 8 uur.

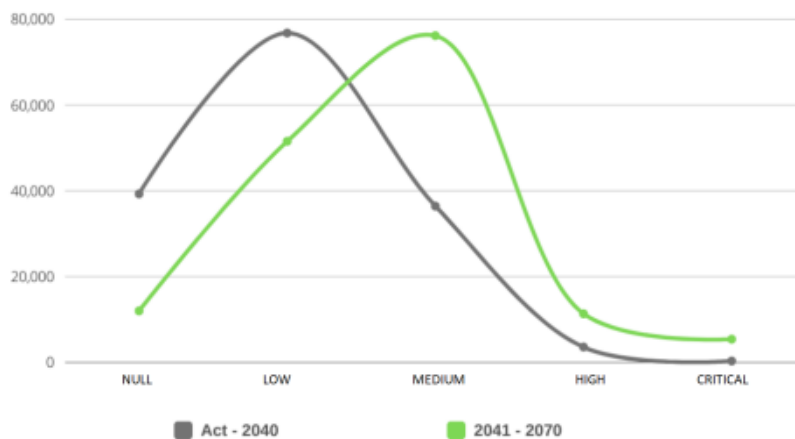
Voor C2000 kan het probleem bij uitval van een mast groter zijn, door het kleinere aantal masten (500+), waarbij een verstoring effect heeft in een groter gebied rondom de mast. De vervangingscyclus van netwerkapparatuur in radionetwerken is relatief kort (5-10 jaar), zeker vergeleken met de periode van klimaatverandering tot 2050 en 2100. In 2050 zal de huidige 5G-apparatuur al meerdere keren zijn vervangen door 6G of 7G. Bij vervanging kan men rekening houden met andere eisen ten gevolge van klimaatveranderingen en duurzaamheid, bijv. via kleinere apparatuur met lager stroomverbruik en beter geschikt tegen hogere temperaturen. Apparatuur is nu reeds ontworpen om te werken bij extreme temperaturen van typisch -20 tot +50 graden.

Mobiele netwerk operators zoals KPN, Odido en VodafoneZiggo en exploitanten van mobiele opstelpunten zoals CellNex zijn zich bewust van klimaatrisico's en rapporteren hierover jaarlijks, zie bijv. 'Environment and Climate Change Report' van CellNex [46] of KPN [47]. Deze bedrijven maken, net als veel andere bedrijven in de sector ICT, gebruik van de generieke methodiek ontwikkeld door de Task Force on Climate-Related Financial Disclosures (TCFD [39]), na 2023 geborgd binnen IFRS [40]. In deze methodiek wordt klimaatgerelateerde risico's én kansen (*risks & opportunities*) van bedrijf, leveranciers en concurrenten meegenomen binnen een bredere, financieel-gedreven risicoanalyse. Op basis van de risicoanalyse en een strategische planning op korte, middellange en lange termijn kunnen financiële middelen worden toegekend om de risico's te verminderen en kansen te verzilveren, zoals energiebesparing en beter presteren dan de concurrentie.

Voorbeeld klimaatrisicoanalyse van CellNex.

Cellnex Nederland is actief sinds 2016 en beheert 4.139 locaties en meer dan 700 radiozenders. De telecommunicatie-infrastructuur van Cellnex in Nederland bestaat uit antennemasten, daken, zendmasten en -netwerken, datacenters en indoor Distributed Antenna System (DAS)-installaties. Cellnex Nederland heeft drie hoofdklanten: Odido, KPN en VodafoneZiggo. In het 'Environment and Climate Change Report' rapport van CellNex uit 2023 is een uitgebreide analyse (voor de periode 2030-2050) opgenomen van klimaatrisico's op basis van klimaatmodellen van IPCC, met zowel i) directe, fysieke risico's van klimaatverandering op de infrastructuur als ii) risico's van de transitie naar klimaatneutrale bedrijfsvoering op basis van wetgeving t.a.v. CO₂-uitstoot, de energietransitie naar net-zero en efficiënter energiegebruik. Cellnex maakt gebruik van een Climate Change Adaptation Plan (CCAP) met acties om toekomstige schade van acute (extreem weer) en chronische klimaatverandering (temperatuurstijging, zeespiegelstijging) te beperken of te voorkomen op de meer dan 150.000 assets (masten, technische gebouwen en data centers) in de 10 landen waar ze actief zijn. Zij maken hierbij

ook een vertaling naar de financiële impact. De analyse (zie Figuur 9), laat de verandering van risico's per land zien voor de periodes 2020-2040 en 2040-2070.



Figuur 9 Assets met de verschillende classificatie van klimaatrisico's voor periode tot 2040 en 2040-2070 [46]

In de periode tot 2040 is slechts voor 2% van de assets sprake van een hoog of kritiek risico (high/critical), waarbij adaptatiemaatregelen nodig zijn; in de periode 2040-2070 zal dit sterk stijgen naar 11%, ofwel meer dan een factor 5.



Figuur 10 Percentage van assets per land met de verschillende classificatie van klimaatrisico's voor periode 2020-2040 en 2040-2070 [46]

Voor de landen in Zuid-Europa (Spanje, Portugal, Italië) en het Verenigd Koninkrijk is er in de periode tot 2040 al sprake van locaties met een hoog of kritisch risico, zie Figuur 10. Voor Nederland is hier pas sprake van in de periode 2040-2070. Acute en chronische fysieke risico's door temperatuur en overstromingen worden als grootste risico's gezien (p. 45 in [46]). Er is door Cellnex een analyse gemaakt van de financiële impact van de fysieke, chronische risico's. Deze analyse laat een beperkte jaarlijkse toename in operationele kosten door extra kosten koeling en 1,6 MEUR verlies op omzet per jaar. De impact op verlies van waarde van assets is aanzienlijk groter en wordt geschat op 26 MEUR per jaar, met name door het toenemende gevaar van overstromingen in kustgebieden. Voor Cellnex geldt dit laatste risico als belangrijkste risico voor Nederland, in Zuid-Europese landen vormen extreem weer, hitte en waterschaarste een groter risico.

In het rapport uit 2024 [48] is de studie uitgebreid met de periode 2070/2100 en zijn klimaatrisico's in drie periodes meegenomen 2020/2040 (kort), 2040/2070 (midden) en 2070/2100 (lang). Deze studie laat een vergelijkbaar beeld zien als in 2023, waarbij de fysieke risico's van klimaatverandering bij zowel een realistisch (SSP2-RCP4.5 +2,5 - 3°C opwarming), als het slechtste scenario (SSP5-RCP8.5 met +4,5-6°C opwarming) toenemen. Het aantal locaties met risico 'high' of 'critical' neemt bij het realistische scenario toe van 4% in 2020/2040 naar 14% in 2070/2100 en van 4% naar 22% bij het slechtste scenario (zie tabel op pagina 159 van rapport Cellnex 2024). In Figuur 11 zijn de klimaatrisico's voor blootstelling aan 8 verschillende klimaatvariabele weergegeven (temperatuur, neerslag, wind, overstroming door zee of rivieren, (bos)brand, landverschuivingen, sneeuw) beschreven voor alle locaties van Cellnex (112.105 in 2024) in de 11 landen in Europa waar ze actief zijn. Het merendeel betreft zendmasten of opstelpunten voor mobiele communicatie en radio. Wind (9%), bosbranden (10%) en sneeuw (12%) vormen de grootste risico's in het realistische scenario met ca. 10% met 'high' of 'critical risk'. In het slechtste scenario vormen extreme temperaturen ook een groter risico, voor 11% i.p.v. 3% van de locaties, en veranderen de andere risico's licht met 1-2%.

SSP2-RCP4.5 - realistic scenario (+2.5-3°C warming)								
Potential risk exposure (null, low, medium, high, critical) by climate variable at Cellnex sites throughout the time period analysed (act-2100) in the realistic climate scenario								
Risk exposure	Temperature	Precipitation	Wind	Flooding from marine origin	Flooding from river origin	Fire	Landslides	Snow
NULL	78%	0%	43%	98%	96%	71%	3%	20%
LOW	12%	7%	24%	0%	0%	5%	48%	40%
MEDIUM	7%	93%	24%	0%	3%	14%	48%	28%
HIGH	3%	1%	9%	1%	1%	9%	1%	10%
CRITICAL	0%	0%	0%	0%	0%	1%	0%	2%
TOTAL	100%	100%	100%	100%	100%	100%	100%	100%
SSP5-RCP8.5 - worst case scenario (+4.5-6°C warming)								
Potential risk exposure (null, low, medium, high, critical) by climate variable at Cellnex sites throughout the time period analysed (act-2100) in the worst-case climate scenario								
Risk exposure	Temperature	Precipitation	Wind	Flooding from marine origin	Flooding from river origin	Fire	Landslides	Snow
NULL	59%	0%	43%	98%	96%	69%	3%	23%
LOW	18%	6%	24%	0%	0%	4%	45%	42%
MEDIUM	11%	93%	24%	0%	3%	14%	51%	25%
HIGH	10%	1%	9%	1%	1%	10%	2%	8%
CRITICAL	1%	0%	0%	0%	0%	2%	0%	1%
TOTAL	100%	100%	100%	100%	100%	100%	100%	100%

Figuur 11 Klimaatrisico's per variabele voor locaties Cellnex in de periode tot 2100 voor twee scenario's [Bron: 2024 Integrated Annual Report, Cellnex]

De risico's verschillen sterk per land, met de grootste risico's voor Italië, Spanje en Portugal en in mindere mate in bijv. Nederland, Ierland of het Verenigd Koninkrijk.

Adaptatie door de overheid

De drie mobiele operators in Nederland zijn aangewezen als aanbieders van vitale infrastructuur, met bijbehorende verplichting rondom continuïteit (Telecomwet, hoofdstuk 11a

en specifiek artikel 11a.3 voor antenne-opstelpunten). Hiermee zijn indirect ook maatregelen tegen klimaatrisico's zoals hitte of extreem weer opgenomen.

Voor het C2000-netwerk is de overheid verantwoordelijk. Het is niet bekend of de overheid zelf ook periodiek een klimaatrisicoanalyse uitvoert voor eigen netwerken (zoals het C2000-netwerk, maritieme netwerken en communicatienetwerken rondom vliegvelden voor de luchtverkeersleiding), inclusief opstelpunten, en maatregelen neemt.

5.2.3 Blootstelling

De kans op hogere temperaturen zal toenemen in Nederland. Er komen meer dagen met extremere temperaturen van boven de 35 graden. Ook zal de uitbreiding van 5G-netwerken en toekomstige technologieën meer zendmasten vereisen voor betrouwbare dekking. Al met al zal dus de blootstelling aan het klimaatrisico toenemen.

Blootstelling van (mobiele) netwerken bij hitte is landelijk, maar kans op uitval per mast is lokaal en incidenteel. Netwerkapparatuur is ontworpen om, zonder koeling, bij extreem hoge temperaturen tot 50 graden te werken. Een van de geïnterviewden partijen gaf aan dat hitte-eilanden in stedelijk gebied zorgen voor een verhoogd risico op te hoge temperaturen van apparatuur en onvoldoende koeling. Deze partij is daarom de temperatuur in alle technische ruimtes gaan monitoren, om problemen tijdig te kunnen identificeren.

Verder zijn er ook ruimtelijke verschillen:

- *Kustgebieden:* Aan de kust is er minder sprake van hitte. Het verwachte aantal tropische dagen langs de kust in 2050 (hoogste scenario) is ca. 3-10 langs de kust en 15-25 in het zuidoosten [Klimaat-effectatlas].
- *Stedelijke gebieden:* Deze gebieden zijn sneller heet door het zogenaamde 'stedelijk hitte-eiland'. Dit komt door bebouwing en infrastructuur die warmte absorberen en vasthouden, door minder groen dat kan helpen bij verkoeling en door menselijke activiteiten als verkeer en industrie.
- *Binnenland:* In het binnenland zijn er relatief meer extreem hete dagen. Bijvoorbeeld in 2100 rond de 17 per jaar (Klimaat-effectatlas [30]).

5.2.4 Gevoeligheid

De gevoeligheid voor hitte is laag, en ook naar de toekomst toe zal dit zo blijven is de verwachting. Er is geen schade bekend van hitte bij masten.

Gevoeligheid voor grootschalige en structurele uitval van apparatuur op masten door hitte lijkt laag, en de gevolgen op dekking bij lokale uitval van een enkele mobiele mast door oververhitting lijkt beperkt.

Nederland ligt in een gematigd klimaat, (langdurige) extreme hitte komt in zuidelijke landen al vaker voor en daar lijkt dit geen structureel probleem. De kans op structurele en brede uitval in Nederland lijkt hiermee vooralsnog klein, apparatuur is onder normale omstandigheden bestand tegen temperaturen tot 50 graden.

5.2.5 Impact

Uitval van masten heeft gevolgen voor de dekkingsgraad. Wanneer zendmasten uitvallen, kunnen gebruikers problemen ondervinden met het maken van telefoongesprekken, het verzenden van berichten en het gebruik van mobiele data. Ook zorgt het voor verhoogde netwerkbelasting van nabijgelegen masten, dit kan resulteren in verminderde netwerkprestaties en lagere (internet)snelheden.

Voor de noodcommunicatie heeft het de grootste impact. Wanneer telecommunicatie-infrastructuur zoals C2000 wordt geraakt kan de communicatie tussen hulpdiensten en de bevolking ernstig worden verstoord.

Uitval en/of verminderde beschikbaarheid van mobiele communicatie heeft met name impact als het gaat om kritische communicatie (mobiele netwerken i.v.m. bereikbaarheid 112 en NL-Alert, en het C2000 netwerk voor hulpverleners) met als gevolg vertraging in hulpverlening.

5.3 Masten en extreem weer

5.3.1 Klimaatdreiging(en)

In paragraaf 4.2 zijn de klimaatrisico's voor de verschillende onderdelen binnen de digitale infrastructuur beschreven.

Er is geen onderscheid gemaakt tussen de contextscenario's 'beperkt risicoverhogend' en 'sterk risicoverhogend'. Er zijn geen secundaire effecten bekend van extreem weer op masten.

5.3.2 Adaptatiemaatregelen huidig beleid

Adaptatiecapaciteit vanuit de sector

Mobiele netwerken bestaan uit een groot aantal masten (ca. 16.000) in de drie mobiele netwerken in Nederland. Incidentele uitval van een mast door extreem weer in één van de drie mobiele netwerken blijft beperkt tot een lokaal effect: verminderde dekking voor abonnees van de getroffen MNO, totdat dit hersteld is. Herstel vindt typisch plaats binnen 4 tot 8 uur.

Voor C2000 kan het probleem bij uitval van een mast groter zijn, door het kleinere aantal masten (500+), waarbij een verstoring effect direct heeft in een groter gebied rondom de mast.

Adaptatie door de overheid

De drie mobiele operators in Nederland zijn aangewezen als aanbieders van vitale infrastructuur, met bijbehorende verplichting rondom continuïteit (Telecomwet, hoofdstuk 11a en specifiek artikel 11a.3 voor antenne-opstelpunten). Hiermee worden indirect ook maatregelen tegen klimaatrisico's zoals extreem weer en hitte afgedwongen.

Voor het C2000-netwerk is de overheid verantwoordelijk. Het is niet bekend of de overheid (Politie) zelf ook periodiek een klimaatrisicoanalyse uitvoert voor het C2000-netwerk, inclusief opstelpunten.

In het Besluit Bouwwerken Leefomgeving (BBL, voorheen het Bouwbesluit) zijn er specifieke eisen opgenomen voor de constructieve veiligheid van masten, waaronder de windbelasting die ze moeten kunnen weerstaan. Masten moeten windkracht 12 aan kunnen. Dit kan gezien worden als preventieve adaptatie.

Innovaties in materialen en ontwerp kunnen de weerbaarheid van apparaten tegen extreme weersomstandigheden verbeteren. Er lijkt echter geen sprake te zijn van specifieke innovatietrajecten ten behoeve van adaptatie voor extreem weer.

5.3.3 Blootstelling

De uitbreiding van 5G-netwerken en toekomstige 6G-netwerken zal betekenen dat er naar verwachting meer zendmasten komen om betrouwbare dekking en capaciteit te blijven garanderen. In die zin zal de blootstelling voor dit klimaatrisico toenemen. Ook zal er vaker sprake zijn van extreme regenval en hagelbuien. Dit zal echter vrij lokaal optreden.

De kans op hoge windsnelheden zal volgens de KNMI'23 klimaatscenario's [8] niet significant toenemen in Nederland.

De landelijke netwerken met masten die worden blootgesteld zijn mobiele netwerken, C2000 en radio en televisie via de ether (DVB-T2). Verder zijn er nog lokale netwerken voor bijv. maritieme communicatie en luchtvaartcommunicatie. Alle apparatuur wordt ongeveer in dezelfde mate blootgesteld, al zijn er nuance verschillen. Zo wordt apparatuur hoger op de mast meer blootgesteld aan wind en hagel dan apparatuur in een kast onder bij de mast.

Verder zijn er ook ruimtelijke verschillen:

- ☐ *Kustgebieden:* Deze zijn meer blootgesteld aan stormvloed en harde wind door de nabijheid van de Noordzee.
- ☐ *Stedelijke gebieden:* Door dichte bebouwing en infrastructuur zouden hier windtunnels kunnen ontstaan.
- ☐ *Binnenland:* Deze zijn iets minder blootgesteld aan stormvloed en zeewind, maar kunnen alsnog te maken krijgen met wind en stormen vanuit andere richtingen.
- ☐ Lokale extreme neerslag en hagel kan in heel Nederland voor komen.

Blootstelling bij extreem weer is lokaal, met kans op verstoring per mast. Alleen bij een overstroming in een gebied is er mogelijk uitval van meerdere masten in een gebied. Dit komt veelal doordat de stroomvoorziening wegvalt of apparatuur preventief wordt afgeschakeld om schade bij kortsluiting te voorkomen. Een lokale noodstroomvoorziening werkt typisch max. 2-3 uur

5.3.4 Gevoeligheid

Er is tot nu toe geen schade bekend van extreem weer bij masten [interview MNO]. De gevoeligheid voor extreem weer, in dit geval stormen, wind, extreme neerslag of hagel is dus laag, en ook naar de toekomst toe zal dit zo blijven is de verwachting.

Stormen van windkracht 12 of hoger komen in Nederland tot nu toe zelden voor [interview MNO]. Naar de toekomst toe worden voor windsnelheden nauwelijks of geen verandering verwacht. Ook voor extreme neerslag en bliksem zijn er op dit moment geen of enkel incidentele, lokale storingen bekend. Er zijn wel voorbeelden bekend vanuit andere landen: zo zorgde de storm Éowyn in januari 2025 in Ierland voor grote problemen o.a. ten gevolge van stroomuitval [49]. Op het hoogtepunt van de storm had 1 op de 3 gebruikers problemen met mobiele dekking door stroomuitval of andere vormen van schade, en ook een dag na de storm hadden meer dan 1 miljoen mensen geen toegang tot een mobiele netwerk.

5.3.5 Impact

Extreem weer vindt meestal heel lokaal plaats, wat maakt dat de impact minder groot zal zijn. Wanneer individuele masten uitvallen zal dat gevolgen hebben voor de lokale dekking. Uitval van masten heeft gevolgen voor de dekkingsgraad. Lokaal kunnen gebruikers problemen ondervinden met het maken van telefoongesprekken, het verzenden van berichten en het gebruik van mobiele data. Ook zorgt het voor verhoogde netwerkbelasting van nabijgelegen masten, dit kan resulteren in verminderde netwerkprestaties en lagere (internet)snelheden.

Voor de noodcommunicatie heeft het de grootste impact. Wanneer netwerken die worden gebruikt voor de kritische communicatie wordt geraakt, zoals mobiele netwerken voor 112 en NL-Alert, en het C2000-netwerk voor hulpverleners, kan de communicatie tussen hulpdiensten en de bevolking lokaal worden verstoord, en de hulpverlening mogelijk worden vertraagd.

5.4 Datacenters en combinatie van hitte en droogte

5.4.1 Klimaatdreiging(en)

In paragraaf 4.2 zijn de klimaatrisico's voor de verschillende onderdelen binnen de digitale infrastructuur beschreven. In deze paragraaf is een uitgebreidere kwantitatieve en - waar mogelijk - kwalitatieve, onderbouwing gedaan van de geselecteerde risico's uit paragraaf 4.3. Bepaalde toelichtingen in onderstaande tekst komen ook voor in paragraaf 4.2.4.

In onderstaande tabel zijn de veranderingen uit KNMI'23 klimaatscenario's [8] voor warme en tropische dagen en het neerslagtekort overgenomen. Dit is van belang voor de klimaatrisico's voor hitte en droogte. In de analyse door TNO zijn alleen de dreigingen tot 2050 meegenomen. De periode tot 2100 is te ver in de toekomst om een goede inschatting te maken van de ICT-infrastructuur. Het aantal warme dagen (>25°C) neemt toe van 28 (Huidig) naar 40 (Beperkt) of 49 (Sterk) in 2050, een toename van ca. 40-80%. Voor tropische dagen (>30°C) is de toename van 5 (Huidig) naar 9 (Beperkt) of 12 (Sterk), een toename van ca. 80-140%.

Klimaatfactor	Bron	Huidig	Klimaatscenario's: Ln=Beperkt, Hd=Sterk			
			2050		2100	
			Beperkt	Sterk	Beperkt	Sterk
Aantal dagen met temp. boven 25°C (zomers)	KNMI'23	28	40	49	40	89
Aantal dagen met temp. boven 30°C (tropisch)	KNMI'23	5	9	12	9	30
Droogte: neerslagtekort groeiseizoen (t.o.v. 1991-2020 gemiddelde) (mm)	KNMI'23/Delta	160	13%	35%	13%	79%

De klimaatrisico's uiteten zich in de volgende directe risico's voor datacenters:

1. Periode van extreme hitte

De vraag naar koeling stijgt significant bij temperaturen boven de 25-30°C, wat de energiebehoefte van datacenters verhoogt. Koeling is zo'n 10-30% van het huidige energieverbruik van een datacenter [34], en bij temperaturen boven de 25°C stijgt ook de watervraag (zie droogte voor verdere uitwerking). Koelelementen zoals ventilatoren worden zwaarder belast en kunnen sneller defect raken. Bij extreme hitte kunnen overbelaste koelsystemen falen, wat leidt tot automatische afschakeling van servers en mogelijk verstoring van digitale diensten, maar er ontstaat doorgaans geen permanente hardware schade [interview Bytesnet].

2. Droogte met restricties op drinkwatergebruik (Schaarste koelwater, bodemdaling)

Naast de toename van hittegolven nemen ook droge periodes toe. Dit kan leiden tot drinkwaterrestricties, die een directe impact hebben op datacenters die gebruik maken van koeling met drinkwater op dagen dat het warmer is dan 25-30°C. 79% van de Nederlandse datacenters gebruikt drinkwater voor koeling [50], en watergebruik is hoog met name op hete dagen. Bij ernstige droogte kan de overheid (en drinkwaterbedrijven) – op basis van de verdringingsreeks bij waterschaarste [51] beperkingen opleggen op het gebruik van drinkwater voor industriële doeleinden, waardoor watergekoelde datacenters onvoldoende koelcapaciteit hebben. Hyperscale datacenters zoals Google en Microsoft in Eemshaven en Middenmeer maken al deels gebruik van alternatieve waterbronnen zoals oppervlaktewater en hergebruikt regenwater. De verwachting is dat het volume van waterconsumptie de komende 5 jaar niet stijgt [50]. Precieze cijfers over het watergebruik in piekmomenten (bij hoge buitentemperatuur) zijn niet beschikbaar. Er zijn wel grote regionale verschillen vanwege de spreiding van datacenters over Nederland [52]. Zo zijn veel colocatie-datacenters en kleinere faciliteiten nog afhankelijk van drinkwater en hebben geen infrastructuur om over te schakelen naar alternatieve bronnen.

5.4.1.1 Secundaire effecten bij extreme hitte

Periodes met extreme hitte hebben direct effect op datacenters doordat meer koeling nodig is. Hierdoor stijgt het elektriciteitsverbruik voor koelsystemen en neemt de vraag naar drinkwater toe bij datacenters die waterkoeling gebruiken. Dit heeft secundaire effecten op zowel de energievoorziening als het drinkwatergebruik. In de verdere analyse zijn de secundaire effecten van klimaat op problemen in lokale of regionale elektriciteitsvoorziening bij hitte niet meegenomen. Er is een grote afhankelijkheid van datacenters van de elektriciteitsvoorziening, en hiervoor worden verschillende adaptatiemaatregelen genomen vanuit de sector.

Voor datacenters is een indicatieve inschatting gemaakt van de toename in watergebruik voor koeling bij een toename van het aantal warme en tropische dagen tot 2050 en 2100. De sector ICT gebruikt jaarlijks minder dan 0,1% van het drinkwater, maar op lokaal niveau is dit percentage hoger en het watergebruik is vooral hoog op hete (en dus wellicht droge) momenten. Indien er geen aanvullende adaptatiemaatregelen worden genomen vanuit de sector zal het drinkwatergebruik dus toenemen, aangezien 79% van de huidige datacenters drinkwater gebruiken (situatie 2024).

Zonder adaptatiemaatregelen zal het watergebruik voor koeling bij temperaturen boven 25°C stijgen met 40-75% in 2050, omdat het aantal warme dagen toeneemt bij beperkt en sterk

scenario. Nieuwe koelsystemen die luchtcooling tot 29°C mogelijk maken, kunnen deze stijging beperken. Zo gebruikt het Microsoft-datacenter in Middenmeer pas watercooling bij temperaturen boven 29,4°C, waardoor het waterverbruik is teruggebracht tot minder dan 5% van het jaar.

In 2050 zal het aantal tropische dagen (boven 30°C) toenemen van 5 naar 9-12, wat het watergebruik in sommige datacenters met een factor 1,8-2,4 laat stijgen. De sector werkt aan maatregelen zoals alternatieve waterbronnen en efficiëntere koelsystemen. Desondanks kan het drinkwatergebruik tijdens piekmomenten aanzienlijk toenemen.

5.4.1.2 Secundaire effecten bij droogte met restricties op drinkwatergebruik

Een langere periode van extreme hitte en droogte kan leiden tot een drinkwatertekort, als effect van droogte. Langdurige droogte leidt namelijk tot een aanzienlijke daling van de grondwaterstand, wat de beschikbaarheid van water voor landbouw en drinkwater vermindert. Droogteperiodes kunnen weken tot maanden aanhouden, wat leidt tot langdurige watertekorten. Een secundair effect voor de sector ICT ontstaat indien er restricties worden opgelegd in het gebruik van drinkwater. Hiermee zal de kans op koelingsproblemen toenemen bij datacenters op dagen boven 25°C. Datacenters kunnen alternatieve waterbronnen gebruiken voor cooling, maar water voor datacentercooling heeft lage prioriteit bij een watertekort, volgens de Verdringingsreeks. In de Verdringingsreeks bij watertekort (Besluit kwaliteit leefomgeving Artikel 3.14 [53]) valt (drink)water voor datacentercooling namelijk in de laatste categorie. Het gevolg van koelwatergebrek is uitschakeling van de servers in het datacenter. Hoewel veel datacenters back-up watervoorraad hebben bedoeld voor kortstondige verstoring van de watertoevoer, is het onduidelijk of deze voldoende is bij langdurige waterbeperkingen.

5.4.2 Adaptatiemaatregelen huidig beleid

De gevoeligheid voor verstoringen door klimaatrisico's is minimaal, en verwaarloosbaar als er door organisaties/bedrijven meerdere datacenters worden gebruikt die geografisch zijn verspreid. Organisaties/bedrijven zijn hiervoor zelf verantwoordelijk en gebruiken daarom voor vitale ICT meerdere datacenters voor hoge beschikbaarheid, bijvoorbeeld via 'twinning', waarbij twee datacenters als één fungeren en elkaars back-up zijn. De overheid, inclusief Defensie, maakt ook gebruik van meerdere datacenters binnen Nederland.

Telecomaanbieders maken typisch gebruik van vier of meer core locaties binnen Nederland. Hyperscalers bieden een zeer hoge beschikbaarheid door gebruik van meerdere datacenter locaties, met regionale en globale zones. Verder zijn andere risico's op technische verstoringen bij datacenters veelal groter dan klimaatgerelateerde verstoringen, zie bijv. [38]. Bij de adaptatiecapaciteit ten aanzien van klimaatrisico's is dit bekeken vanuit de sector zelf en vanuit de overheid. Datacenters maken onderdeel uit van de private sector, waarbij financiële afwegingen (op korte tot middellange termijn) van datacenter aanbieders een belangrijke rol spelen, ook ten aanzien van risico's en maatregelen. Bedrijven in de sector ICT zien adaptatiemaatregelen als een risico met financiële afwegingen, terwijl de overheid zich richt op lange termijn beleidsmaatregelen. Deze zijn gericht op het verkleinen van de blootstelling aan, gevoeligheid voor of impact van risico's op de lange termijn.

Daarnaast is er een adaptatie van datacenters vanuit duurzaamheid, deels uit financieel oogpunt, deels vanuit wetgeving of afspraken binnen de sector. Een aanbieder als Google heeft als doel om tegen 2030 een netto nul uitstoot van CO₂ te bereiken voor alle eigen activiteiten en heeft als doelstelling alle kantoren en datacenters te laten werken op 24/7 CO₂-neutrale energie. In 2023 kondigde Google een overeenkomst aan met Eneco om de energievoorziening (van 153 MW) van de datacenters verder CO₂-neutraal te maken en een lange-termijn overeenkomst met het bedrijf EDP Renewables (EDPR) voor de afname van schone energie van een zonne-energiecentrale die EDPR in Nederland ontwikkelt. De nieuwe locatie in Winschoten kan de restwarmte van het koelproces van het datacenter opvangen en overdragen aan geschikte toekomstige afnemers. Het opvangen van de warmte van het datacenter is een kans voor energiebesparing en draagt lokaal bij aan de energietransitie. De locatie wordt ook voorzien van zonnepanelen op het dak [54]. Andere aanbieders werken aan vergelijkbare oplossingen. Ook zien we dat drinkwaterbedrijven voor nieuwe locaties geen drinkwater voor koeling meer willen leveren, waardoor men gedwongen wordt alternatieve waterbronnen te gebruiken (opslag regenwater in bassin, oppervlaktewater).

5.4.2.1 Adaptatiecapaciteit sector ICT bij extreme hitte

Vanuit de sector ICT zijn of worden al verschillende adaptatiemaatregelen genomen. Hieronder zijn de belangrijkste genoemd, die voor een belangrijk deel ook wordt bepaald door Europese en landelijke wetgeving van de overheid:

Preventieve adaptatie: vanuit duurzaamheid/ecologische footprint zijn er vanuit de sector verschillende initiatieven om energieverbruik van datacenters te verminderen. Ook richten initiatieven zich op verbeterde oplossingen voor koeling die minder of zelfs geen gebruik maken van drinkwater. Denk hierbij aan gesloten koelsystemen, opslag en gebruik van regenwater of oppervlaktewater (zie voorbeelden hyperscale datacenters Google en Microsoft in Nederland), en alternatieve koeltechnologie (zoals *liquid cooling*). Voor energievoorziening wordt er gebruik gemaakt van UPS, en (diesel)aggregaten. Op de hightech Campus Eindhoven is een oplossing die gebruikt maakt van waterstof als energiebron voor noodaggregaten. Er zijn ook al voorbeelden van datacenters die volledig gebruik maken van waterstof voor elektriciteitsvoorziening [55]. Bedrijven/organisaties zijn zelf verantwoordelijk voor voldoende redundantie in vitale ICT-applicaties. Hyperscalers kennen een zeer hoge mate van redundantie (tot N+4), colocation providers bieden ook een hoge mate van redundantie (minimaal N+1), met toenemende mate van redundantie regionaal/nationaal/internationaal. Voor het grote aantal kleinere datacenters (single tenant, 5.231 in 2024 [50]) is niet duidelijk welke mate van redundantie zij hanteren voor hun datacenter(s) en back-up.

Reactieve adaptatie: datacenters hebben noodplannen om in geval van een calamiteit, zoals uitval van koelsystemen of stroomvoorziening bij extreme hitte, back-up te hebben voor elektriciteit (UPS en noodaggregaten en/of koeling (watervoorraden aanvullen)).

Trend:

De trend in de datacentersector is een groeiend aantal datacenters, meer investeringen in redundantie en adaptatie op gebied van duurzaamheid. Dit omvat een mix van energiebronnen richting CO₂-neutraliteit, efficiënter energie- en watergebruik en een verminderde afhankelijkheid van drinkwater. Hyperscalers lopen hierin voorop, mede door

strengere regelgeving. Daarnaast leidt de verschuiving van enterprise naar colocatie en van colocatie naar (hybride) cloud oplossingen van hyperscalers tot verdere versterking van deze ontwikkelingen. Hierdoor wordt verwacht dat de impact van klimaatrisico's op uitval afneemt, dankzij hogere redundantie en verminderde afhankelijkheid van drinkwater voor koeling.

(On)mogelijkheden voor adaptatie:

Aanvullende wetgeving voor datacenters is met name gericht op duurzaamheid om energie- en watergebruik te beperken en een duurzame energiemix (CO₂-neutraal). Dit zorgt ervoor dat bestaande en nieuwe datacenters investeren in energie- en koelsystemen. De adaptatiecapaciteit verschilt, mede door wetgeving, ook tussen enterprise, colocatie en hyperscale datacenters. Hyperscale datacenters sluiten – door de grote vraag - veelal directe overeenkomsten met energieleveranciers voor directe levering van duurzame energie uit zon en wind. In de VS zie je inmiddels de neiging van AI datacenter providers om hun eigen energiecentrales te bouwen (en dan vooral kerncentrales i.v.m. hun leveringszekerheid) die specifiek zijn voor de snelle groei in energieverbruik van datacenters. Deze 'trend' is vergelijkbaar met het aanleggen van 'eigen' onderzeese datakabels door de oceanen door hyperscalers in de afgelopen twee decennia. Door de schaalgrootte van de hyperscalers en financiële middelen van Amerikaanse BigTech bedrijven dat het bouwen van 'eigen infrastructuur' voor elektriciteit en datakabels haalbaar is. Voor de veel kleinere enterprise en colocatiedatacenters is dit niet mogelijk. Daarnaast gebruiken de hyperscale datacenters in Eemshaven en Middenmeer géén drinkwater voor koeling, maar regenwater of oppervlaktewater. Dit in tegenstelling tot colocatie datacenters waarvan 79% drinkwater gebruikt voor koeling. Investerings in deze duurzame oplossingen voor energie- en watergebruik door hyperscale datacenters zijn door de schaalgrootte mogelijk. Voor enterprise en colocatie datacenters lijkt adaptatie hierdoor moeilijker, en is samenwerking of een gezamenlijke aanpak binnen hubs/clusters mogelijk nodig die er in Nederland zijn.

5.4.2.2 Adaptatiecapaciteit overheid bij extreme hitte

Vanuit de overheid is er géén specifiek beleid dat direct gericht is op het verkleinen van klimaatrisico's voor datacenters. Er is wel beleid en wetgeving voor bestaande en (nieuwe) datacenters. In een kamerbrief (met bijlagen) van 21 november 2024 over datacenters in de Nederlandse digitale economie [41] wordt toegelicht wat de huidige visie, beleid en wetgeving is. Enkele punten uit deze kamerbrief zijn hieronder toegelicht:

Datacenters zijn een belangrijk onderdeel van de digitale infrastructuur en daarmee van groot belang voor het innovatie- en verdienvermogen van Nederland. Tevens hebben zij een rol bij de borging van de (digitale) open strategische autonomie.

Alle economische activiteiten in Nederland zijn onderworpen aan regelgeving, ook datacenters. Er zijn directe en indirecte kaders (incl. normeringsopties voor ruimtelijke ordening en impact op het milieu, en bestaande randvoorwaarden en standaarden met betrekking tot datacenters. Deze bieden mogelijkheden om deze sector te reguleren. De kaders zijn met name gericht op verbeteringen van duurzaamheid (energieverbruik, - efficiëntie, hergebruik) en impact op milieu (bijv. vergunningen voor lozing van koelwater op oppervlaktewater). Voorbeelden van directe en indirecte kaders zijn:

Vanuit het kabinet bestaat geen stimuleringsbeleid voor de vestiging van datacenters.

Initiatieven voor groei of nieuwvestiging van datacenters, of clustering daarvan in bijvoorbeeld de vorm van industriecampussen, moeten uit de regio of de sector komen. Er bestaat een dilemma tussen enerzijds de wens om in Nederland de digitale infrastructuur van

wereldklasse te behouden of te versterken en anderzijds de beperkingen op het vlak van energie, koelwater en ruimte. Om deze reden hebben verschillende overheidslagen beperkingen ingesteld voor de vestiging van nieuwe datacenters. Hyperscale datacenters (groter dan 10 hectare en met een aansluitvermogen van 70 Megawatt of meer) hebben grote impact op de ruimte en transportcapaciteit van energie. Daarom heeft het Rijk besloten om realisatie van nieuwe hyperscalers te verbieden, met uitzondering van twee bestaande gebieden in Nederland.

De volgende adaptatiemaatregelen vanuit het beleid, gericht op het verkleinen van de blootstelling aan, gevoeligheid voor of impact van risico's zijn onderkend:

Preventieve adaptatie

Nationale en Europese wetgeving vanuit duurzaamheid leidt tot investeringen in datacenters voor energie- en koelsystemen, die de klimaatrisico's van hitte en droogte verkleinen. Denk hierbij aan innovaties in koelsystemen, die minder of niet afhankelijk zijn van waterkoeling, bijv. waterkoeling vanaf hogere buitentemperaturen, *liquid cooling*, of waterkoeling via gesloten systemen of via opgevangen regenwater. Hierdoor worden datacenters minder afhankelijk van (drink)water of oppervlaktewater en het risico op (drink)waterrestricties bij periodes van droogte.

Wetgeving vanuit duurzaamheid en ruimtelijke ordening kan ook leiden tot het verplaatsen van datacenters uit Nederland naar meer noordelijke landen. Omgekeerd kan Nederland aantrekkelijker worden als vestigingslocatie ten opzichte van Zuid-Europese landen.

Reactieve adaptatie

Vanuit de overheid zijn er geen reactieve maatregelen tegen klimaatrisico's, anders dan de noodzakelijke maatregelen voor telecomaانبieders t.a.v. continuïteit in de telecomwet (hoofdstuk 11a, artikel 11a.1 lid 2) en de Wvke voor vitale aanbieders. Hierin zijn generieke eisen opgenomen t.a.v. continuïteit, niet specifiek gericht op maatregelen bij calamiteiten als gevolg van klimaatrisico's.

Daarnaast zijn afnemers van ICT-diensten zelf verantwoordelijk om weerbaar te zijn tegen verstoringen en keteneffecten van hun vitale ICT-functies te beperken. De Nederlandse Rijksoverheid maakt zelf gebruik gemaakt van vier geografisch gescheiden datacenters, en heeft het aantal datacenters teruggebracht van 60 naar 4, waarmee een kostenbesparing wordt behaald door schaalgrootte, maar ook de continuïteit wordt verbeterd door meer uniformiteit t.a.v. continuïteit van datacenters, ook t.a.v. klimaatrisico's.

Trend

Er zijn twee belangrijke trends, namelijk a) de transitie binnen datacenters en de sector ICT naar klimaatneutraal (zie Actieplan Duurzame Digitalisering) en b) toenemende aandacht voor digitale infrastructuur als vitale functie (NIS). Door de transitie worden nieuwe investeringen gedaan in verbeterde oplossingen t.a.v. stroomvoorziening en koeling, met een verminderde kans op uitval door klimaatrisico's. Door het inzicht van het toenemende belang van digitale infrastructuur als vitale functie en aanvullende wetgeving (NIS, Vitaal) komt er meer aandacht voor continuïteit van de digitale infrastructuur bij organisaties/bedrijven. Keteneffecten bij uitval van individuele datacenters zijn moeilijk in te schatten, maar kunnen wel voor grote maatschappelijke ontwrichting zorgen als dit bijv. leidt tot uitval van vitale communicatievoorzieningen.

(On)mogelijkheden voor adaptatie: huidige beleid en wetgeving

Rondom hyperscalers is er landelijke wetgeving die het voor gemeenten onmogelijk maakt om nieuwe locaties aan te wijzen voor hyperscale datacenters.

5.4.2.3 Adaptatiecapaciteit sector ICT bij droogte met restricties op drinkwatergebruik

Datacenters in Nederland verbruiken relatief weinig drinkwater op jaarbasis: 0,089% van totaal in Nederland en 0,3% van zakelijke gebruik. [56] 62% van de leden van Dutch Data Center Association (DDCA) verwachten voor de komende 5 jaar dat het watergebruik gelijk zal blijven, 14% verwacht een toename, de overige 24% een (sterke) afname [57].

De gevraagde leveringscapaciteit per uur op warme dagen kan wel hoog zijn, maar is klein wat betreft levering per jaar [2021 [52]. Drinkwaterbedrijf PWN geeft aan dat industriële klanten samen op jaarbasis 0,6% van de totale waterproductie afnemen voor koeling (650.000 m³). Drinkwaterbedrijven zoals PWN geven aan dat drinkwater op termijn alleen nog moet worden gebruikt voor menselijke consumptie en andere hoogwaardige toepassingen.

Preventieve adaptatie

Er wordt aan alternatieven gewerkt zoals door hyperscalers:

- ☐ Duurzame koeling bij datacenters Middenmeer:
 - Op het bedrijventerrein Agriport in Middenmeer hebben Google en Microsoft elk een datacenter. De datacenters in Middenmeer maken gebruik van vrije luchtkoeling (Free Air Cooling), waarbij warmte via een warmtewisselaar wordt afgegeven aan de koudere buitenlucht. Pas als de buitentemperatuur boven 25 graden stijgt, komt er water aan te pas. Water wordt dan verneveld en verdampt, zodat de inkomende buitenlucht afkoelt en beter warmte opneemt. Op zulke dagen kan de waterinname hoog zijn. Gemiddeld telt Nederland 26 zomerse dagen met een temperatuur boven 25 graden. Overigens mag de temperatuur in de nieuwste generatie datacenters oplopen tot 29 graden. Particulier nutsbedrijf ECW Energy heeft een systeem operationeel om regenwater van de daken van datacenters in Middenmeer op te vangen, te zuiveren en ondergronds op te slaan. Op zomerse dagen kan het voorzien in de vraag naar koelwater.
- ☐ Industriewater als alternatief in Eemshaven:
 - North Water, de joint-venture van Waterbedrijf Groningen en Evides Industriewater biedt ook een alternatief aan het Google-datacenter in de Eemshaven via industriewater. Op het terrein van rioolwaterzuiveringsinstallatie Garmerwolde aan het Eemskanaal is een installatie gebouwd voor de productie van industriewater, waarbij water uit het Eemskanaal wordt opgewerkt tot een kwaliteit die voldoet aan de specificaties. Google heeft als *launching customer* bijgedragen aan de ontwikkeling. Het datacenter in de Eemshaven maakt gebruik van open koeltorens waarbij het jaarrond water wordt toegevoegd.
- ☐ Afgekeurd hyperscale datacenter in Zeewolde:
 - De grootste hyperscale van Nederland stond gepland op bedrijventerrein Trekkersveld in Zeewolde (166 ha voor vijf hallen met servers). De Raad van State oordeelde in september 2023 dat het bestemmingsplan voor zo'n hypermodern datacenter onuitvoerbaar is. Voor dit hyperscale datacenter heeft drinkwaterbedrijf Vitens aangegeven geen drinkwater voor koeling en luchtbevochtiging te leveren. In de vergunningaanvraag was gebruik van oppervlaktewater uit de nabijgelegen Hoge Vaart voorzien.

De datacenters 'produceren' in bovenstaande voorbeelden meer water dan ze daadwerkelijk gebruiken en worden zo uiteindelijk 'water-positief'. Verder zijn drinkwaterbedrijven niet meer bereid om drinkwater te leveren aan nieuwe (hyperscale) datacenters voor koeling.

Overige datacenters:

- Gebruik alternatieve waterbronnen:
 - 79% van de datacenters maakt gebruik van drinkwater voor koeling, 21% van industrieel water. Uit de gegevens van DDCA 2024 blijkt dat er nog geen datacenters zijn die gebruik maken van oppervlaktewater, regenwater of hergebruik van water. De optie van het verzamelen en opslaan van oppervlaktewater, zoals regen is volgens DDCA een optie die het meest geschikt lijkt voor hyperscale datacenters die op relatief grote campussen opereren, met veel potentieel voor verzameling. Voor colocationdatacenters kan het een grotere uitdaging zijn volgens DDCA.
- Europese initiatieven voor waterbesparing:
 - Het Climate Neutral Data Centre Pact (CNDCP), een zelfregulerend initiatief ondertekend door 74 datacenterexploitanten en 23 verenigingen, heeft voorgestelde meetmethoden voor waterbesparing aan de Europese Commissie gepresenteerd. Zij stellen een limiet voor van 0,4 l per kWh.
 - Vanuit duurzaamheid is er momenteel Europese wetgeving (Energy Efficiency Directive, EED, EU/2023/1791) met daarin ook richtlijn voor energie-efficiënte van datacenters, en voor watergebruik. Dit zal bijdragen tot efficiënter gebruik van water.
- Innovaties in waterbesparing:
 - De industrie zoekt hierdoor zelf naar manieren om het waterverbruik te minimaliseren en de afhankelijkheid van drinkwater te verminderen. Door de Stichting DDCA is een white paper [57] opgesteld over mogelijkheden tot het verminderen van watergebruik om het drinkwatergebruik terug te dringen. Een voorbeeld van een duurzaam initiatief is een oplossing, dat lineaire koelsystemen omzet in circulaire systemen. Met een chemicaliënvrije oplossing wordt water behandeld en herhaaldelijk gebruikt binnen het datacenter. Deze aanpak kan de watervoetafdruk met 40% verminderen en het waterverbruik met wel 95%.

Reactieve adaptatie

Datacenters hebben noodplannen om in geval van een calamiteit back-up te hebben voor elektriciteit of koeling. Daarnaast is gefaseerde afschakeling van datacenter workloads mogelijk.

Trend

Het gebruik van drinkwater voor koeling is laag (0,1% op jaarbasis), met lokale verschillen en meer vraag op piekmomenten. Het gebruik van drinkwater voor koeling door datacenters is nog steeds hoog (79% in 2024), een afname in de komende jaren is niet voorzien, maar ook geen toename [50].

(On)mogelijkheden voor adaptatie

Om over te stappen naar alternatieve bronnen voor koeling zijn investeringen en vergunningen nodig. De huidige 'waterpositieve' oplossingen voor de hyperscale datacenters zouden ook gerealiseerd kunnen worden voor hubs/clusters van datacenters of andere grootgebruikers van water. Dit vergt lokale afstemming tussen meerdere partijen en is ook afhankelijk van de beschikbaarheid van oppervlaktewater uit kanalen/rivieren:

- Leverancier industrieel/gefilterd water uit oppervlaktewater, of waterbedrijven (industrieel water)
- Primaire afnemers water (datacenters, industrie)

- ☐ Secundaire afnemers water (bijv. tuinbouw/landbouw);
- ☐ Overheid, vergunningen voor gebruik

5.4.2.4 Adaptatiecapaciteit overheid bij droogte met restricties op drinkwatergebruik

Adaptatiemaatregelen vanuit het beleid, gericht op het verkleinen van de blootstelling aan, gevoeligheid voor of impact van risico's.

Preventieve adaptatie

Het beleid van de overheid is gericht op zuiniger gebruik van drinkwater. Voor zakelijke gebruikers (datacenters) betekent dit hergebruik en het circulair maken van waterstromen en om laagwaardig gebruik van drinkwater tegen te gaan. In de periode 2021-2026 werkt de overheid dit verder uit werkt in de maatregelen.

In opdracht van het Min I&W is een pilot uitgevoerd in het Westelijk havengebied van Rotterdam met 'Waterprofielen industrie' om te zien hoe de 'verdringingsreeks' regionaal in de praktijk kan worden toegepast door alle betrokken partijen binnen overheid en industrie [58]. De pilot was het vervolg op een aanbeveling van de Beleidstafel Droogte. De Beleidstafel Droogte heeft in 2019 aanbevolen om het instrument 'waterprofiel' uit te werken. Dit met als doel om informatie over industrieel watergebruik beter te ontsluiten en daarmee de kwaliteit van de besluitvorming over de waterverdeling en het waterbeheer (voor zover relevant voor de industrie) te verbeteren. In het rapport wordt aangegeven dat er ruimte voor maatwerk nodig is: *"indien sprake is van (dreigend) watertekort wordt door de waterbeheerder per situatie bekeken welke prioriteit binnen categorie 3 en 4 voor moet gaan. Hierbij is het streven naar minimalisering van de maatschappelijke en economische schade leidend"*. [58] Datacenters zijn geen grootgebruikers van water, maar afnemers van drinkwater of industrieel water voor koeling.

Reactieve adaptatie

De mogelijke restricties op drinkwatergebruik zijn in Nederland nog nooit toegepast op (laagwaardig) drinkwatergebruik. Mogelijk dat dit in de toekomst wel noodzakelijk wordt door klimaatverandering.

Trend

Op termijn wordt een trend voorzien dat laagwaardig gebruik van drinkwater voor koeling niet meer wordt toegestaan voor nieuwe datacenters.

(On)mogelijkheden voor adaptatie

Overstap naar alternatieven is voor sector ICT (datacenters) sterk afhankelijk van financiële haalbaarheid, het is nu niet haalbaar voor individuele datacenters, alleen voor hyperscalers. Beleid en wetgeving bepalen de snelheid van deze overstap voor met name de kleinere colocatie datacenters.

Landelijk of lokaal beleid kan ook zorgen dat NL minder aantrekkelijk wordt voor datacenters/hyperscalers, waardoor internationale partijen uitwijken naar andere landen (binnen FLAPD (tier-1) , of naar opkomende steden/regio's (tier 2).

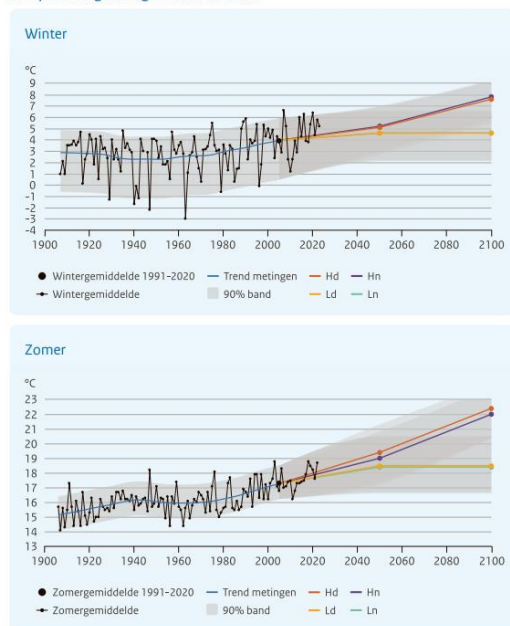
Toekomst

- ☐ Versnelde overstap van laagwaardig gebruik van drinkwater voor koeling naar industrieel water voor koeling
- ☐ Hogere prioriteit drinkwatergebruik voor koeling door datacenters, landelijk of lokaal i.v.m. keteneffecten

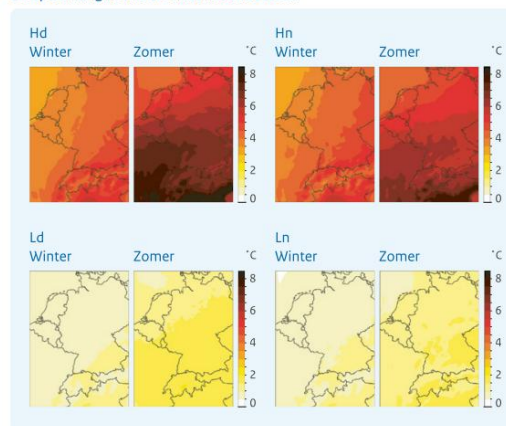
5.4.3 Blootstelling bij extreme hitte

Periodes met extreme hitte zullen **landelijk** zijn en impact hebben op alle datacenters in Nederland. Er zijn wel duidelijk regionale verschillen binnen Nederland met hogere maximumtemperaturen in Oost- en Zuid-Nederland en in stedelijke gebied, zie Figuur 12. Datacenters in de regio Amsterdam, Rotterdam en Groningen hebben minder vaak te maken met tropische dagen ($>30^{\circ}\text{C}$) of extreem warme dagen ($>35^{\circ}\text{C}$), zie Figuur 13. Het aantal tropische dagen varieert sterk over Nederland, met gemiddeld 12 dagen in Nederland in het hoogste scenario in 2050, maar minder dan 5 tropische dagen in het noordwesten en meer dan 20 in het zuiden (Zuidoost Brabant, Limburg).

Winter- en zomertemperatuur
De opwarming is het grootst in de zomer

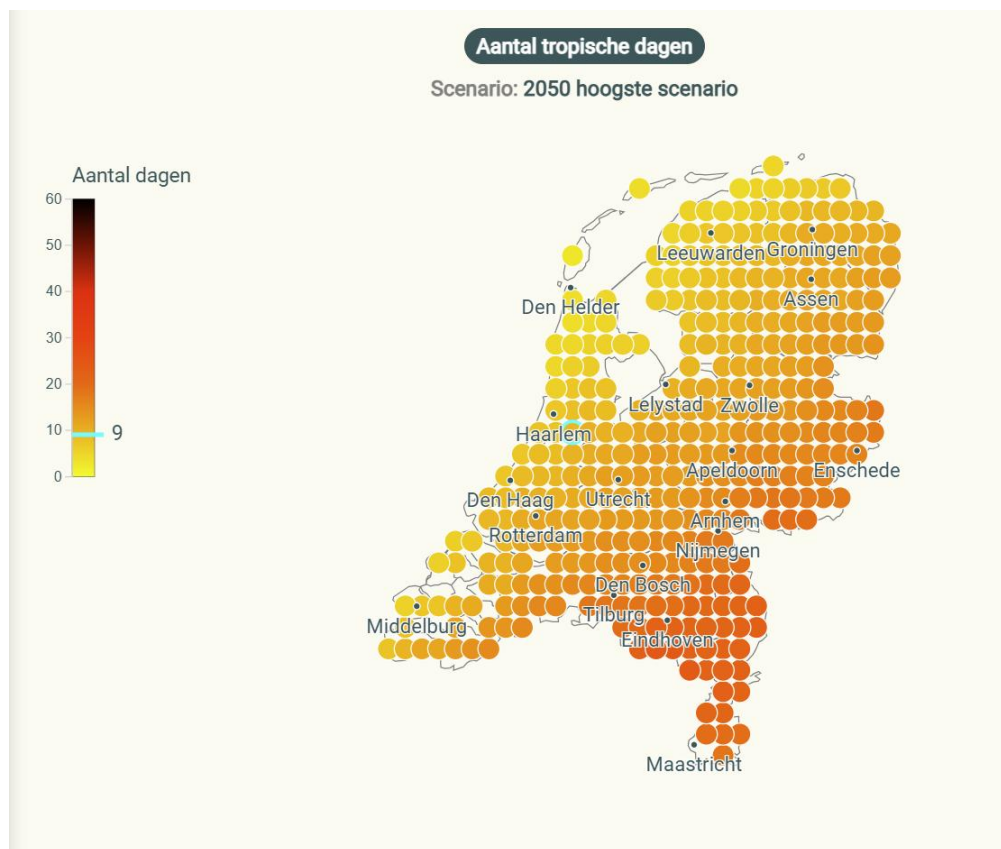


Temperatuur in West-Europa
De opwarming neemt toe naar het zuidoosten



Figuur 9. Temperatuurverandering in West-Europa, in de winter en de zomer rond 2100, volgens de vier KNMI'23-klimaatsscenario's.

Figuur 12 Winter- en zomertemperatuur, landelijk gemiddeld: waarnemingen zwart en de vier KNMI'23-klimaatsscenario's (2050 en 2100, in vier kleuren) (Bron: KNMI'23, figuur 8 in [8])



Figuur 13 Aantal tropische dagen in scenario Hoog 2050. (Bron: Klimateffectatlas [30])

Ook binnen Europa zijn er grote verschillen en periodes met extreme hitte zullen vaker optreden richting het Zuidoosten van Europa. Datacenters in deze regio hebben hierdoor een groter risico. Google heeft momenteel bijv. zes hyperscale datacenters in met name het Noordwesten van Europa: twee in Nederland, en één in vier andere landen (België, Ierland, Finland en Denemarken) en verder drie in ontwikkeling in Nederland, Noorwegen en het Verenigd Koninkrijk [59]. Deze datacenters zijn dus allen gelegen in gebieden met een gematigd zeeklimaat. Microsoft heeft zijn datacenters meer verspreid over heel Europa [60]. Datacenters in het zuidoosten van Europa zullen dus vaker worden blootgesteld aan extreme hitte, met gemiddelde temperatuurstijgingen in de zomer tot meer dan 8°C in 2100 in het hoogste klimaatscenario.

Blootstelling bij droogte met restricties op drinkwatergebruik

Bij restricties op drinkwatergebruik is de aanname dat deze **regionaal** zullen zijn, dus per drinkwaterbedrijf. Hiermee is de blootstelling op dit risico voor datacenters regionaal. In Nederland zijn 10 drinkwaterbedrijven met 221 winningen (exclusief noodwinningen) waarvan 55% uit grondwater, 40% uit oppervlaktewater en 5% uit oevergrondwater [61]. De kans op restricties per drinkwaterbedrijf/gebied zijn niet bekend en daarom niet verder uitgewerkt in de impact op het aantal datacenters per regio.

5.4.4 Gevoeligheid

Datacenters zijn in belangrijke mate afhankelijk van energie- en koelsystemen. Volgens het Uptime Intelligence rapport “Annual outage analysis 2025” [38] had 53% van de respondenten in de afgelopen drie jaar een storing, een daling ten opzichte van 2022 (60%) en 2021 (69%). Slechts 9% van de storingen in 2023 werd als ernstig (*severe* of *serious*) beschouwd, wat een verbetering is ten opzichte van eerdere jaren. 54% van de storingen werd veroorzaakt door stroomuitval en 13% door problemen met koeling. Andere oorzaken zijn uitval van IT systemen (hardware/software) of uitval van netwerken. In het rapport [38] zijn de 10 grootste incidenten in 2024 en 2025 beschreven, waarvan 3 wereldwijd, 5 in de VS, 1 in het VK en 1 in Singapore. In geen van deze gevallen was klimaatverandering de achterliggende oorzaak, ransomware aanvallen (3x) en software- of configuratiefouten na een update (6x) waren de belangrijkste oorzaken. In 1 geval was de ontplofing van een lithium-ion batterij de oorzaak en dit leidde tot schade door de hoge temperaturen en waterschade door blussen van een brand.

Datacenters investeren continue in redundantie van energie- en koelsystemen in datacenters om verstoringen te verminderen, wat zich uit in de daling van ernstige storingen in 2024 t.a.v. 2021. De kosten van uitval kunnen oplopen tot meer dan één miljoen dollar bij een ernstige uitval. Menselijke fouten zijn vaak een oorzaak, verantwoordelijk voor 2/3 tot 4/5 van de storingen.

Gevoeligheid bij extreme hitte

Datacenters zijn goed voorbereid op koelingsproblemen, met voldoende koelcapaciteit voor de ruimte. Alleen bij ernstige storingen in redundante systemen kan de koelcapaciteit tijdelijk onvoldoende zijn, wat kan leiden tot het uitschakelen van servers. Toekomstige datacenters worden ontworpen om ook bij extremen boven 40°C voldoende koeling te bieden. Uitval door koelproblemen tijdens een hittegolf komt (zeer) incidenteel voor. In Londen hadden Google en Oracle op 19 juli 2022 te maken met uitval van hun datacenters tijdens de hittegolf, waarbij de temperaturen stegen tot een recordhoogte van 40°C [62]. Het probleem werd veroorzaakt door gelijktijdige uitval van meerdere, redundante koelsystemen. Google heeft een gedetailleerde toelichting gegeven op de regionale impact op een deel van de klanten, de oorzaak (uitval koelsysteem, afschakeling datacenter, menselijke fouten) en de duur. De hersteltijd was vier uur voor koeling en 18 uur voor clouddiensten [63]. Andere uitvalgevallen werden veroorzaakt door extreem weer zoals bliksem, stormen of natuurbranden, wat bijvoorbeeld resulteerde in uitval van de stroomvoorziening of blokkade van wegen voor personeel.

Gevoeligheid bij droogte met restricties op drinkwatergebruik

79% van de datacenters maakt gebruik van drinkwater voor koeling. Restricties op drinkwatergebruik hebben hierdoor in een periode met temperaturen boven 25°C direct impact op datacenters. De hyperscale datacenters in Middenmeer en Eemshaven maken géén gebruik van drinkwater voor bevochtiging en koeling, en zijn dus niet gevoelig voor restricties op drinkwatergebruik.

5.4.5 Impact bij extreme hitte

De impact voor eindgebruikers zal nihil/minimaal zijn. Uitval van datacenters zal zich beperken tot incidenten die typisch binnen 24 uur zijn opgelost. Door de redundantie in datacenters (meerdere datacenters, verspreid binnen Nederland of Europa) zal de impact nihil/minimaal zijn. Ook voor de overheidsdatacenters (ODC) lijkt dit het geval.

De impact voor datacenters zelf is ook beperkt: een toename van investeringen in koelsystemen met meer capaciteit voor toekomstige extremen, meer duurzame oplossingen voor koeling en de kosten bij herstel van uitval van koelsystemen. De financiële impact voor de exploitant van het datacenter bij grotere incidenten kan wel oplopen tussen 100 kEUR en 1 MEUR per incident [38].

De impact neemt verder af als datacenters geografisch verspreid zijn binnen Europa of wereldwijd. De impact lijkt hiermee het minste voor globale spelers, zoals de cloud providers Amazon, Google en Microsoft. Zij beschikken over meerder hyperscale datacenters binnen een regio (EMEA) en/of wereldwijd met een zeer hoge mate van redundantie door gebruik van zonering in datacenters.

Er zijn geen cascade-effecten voorzien aangezien de directe impact al nihil/minimaal is.

Impact bij droogte met restricties op drinkwatergebruik

De impact zal bij een landelijke restrictie op drinkwatergebruik voor laagwaardig gebruik groot zijn, aangezien dan **alle** datacenters in Nederland, inclusief centrale locaties van vitale telecomaandieners en datacenters van overheid, waarschijnlijk koelproblemen krijgen en gedwongen worden om af te schakelen als luchtkoeling onvoldoende is bij temperaturen boven 25°C.

De daadwerkelijke impact voor individuele datacenters is afhankelijk van de preventieve en/of reactieve adaptatiemaatregelen van individuele datacenters en eventuele noodmaatregelen voor deze bijzondere omstandigheden. Noodplannen van datacenters kunnen mogelijk voorzien in het tijdelijk gebruik van alternatieve oplossingen voor koeling als men niet kan beschikken over drinkwater.

De cascade-effecten zijn naar verwachting zeer groot, en toenemen als er meer en meer datacenters moeten afschakelen door koelingsproblemen. Uiteindelijk komen alle sectoren in Nederland tot stilstand.

5.5 Datacenters en overstromingen

5.5.1 Klimaatdreiging(en)

In paragraaf 4.2 zijn de klimaatrisico's voor de verschillende onderdelen binnen de digitale infrastructuur beschreven. In deze paragraaf is een uitgebreidere kwantitatieve en - waar mogelijk – kwalitatieve onderbouwing gedaan van de geselecteerde risico's uit paragraaf 4.3. Bepaalde toelichtingen komen hierdoor ook voor in paragraaf 4.2.4.

Grote delen van ons land liggen onder zeespiegelniveau verschillende grote rivieren stromen door ons land richting de zee. Overstromingsgevaar komt dus niet alleen vanuit de zee, maar ook vanuit hoogwater in de rivieren door extreme neerslag. Piekaftoeren en het breken van de dijken kunnen voor problemen zorgen.

Deze analyse beschrijft de klimaatdreigingen en de resulterende risico's in twee contextscenario's voor 2050 en 2100: 'Beperkt risicoverhogend' (Ln: lage klimaatverandering, natte omstandigheden) en 'Sterk risicoverhogend' (Hd: hoge klimaatverandering, droge omstandigheden). Hierbij wordt tevens aanvullende informatie uit het Hn-scenario (hoge klimaatverandering, natte omstandigheden) meegenomen voor risico's gerelateerd aan wateroverlast en waterveiligheid. Door deze brede benadering ontstaat een goed beeld van de mogelijke toekomstige ontwikkelingen en de impact op datacenters. In dit factsheet wordt uitsluitend ingegaan op risico's die verband houden met extreme neerslag en overstromingen.

Klimaatdreiging(en) contextscenario 'beperkt risicoverhogend'

In het scenario van beperkt risicoverhogende klimaatverandering worden de belangrijkste risico's veroorzaakt door een toename van neerslag, een beperkte stijging van de zeespiegel en een toename van piekafvoeren in rivieren. De zeespiegelstijging wordt geschat op 16-34 cm in 2050 en 26-73 cm in 2100. Dit kan leiden tot verhoogde overstromingsrisico's in kustgebieden en uitdagingen in het waterbeheer van polders en laaggelegen stedelijke gebieden.

Voor 2050 wordt verwacht dat er meer dagen zullen zijn met extreme neerslag (>20 mm per dag), wat leidt tot een grotere kans op wateroverlast in stedelijke gebieden en een verhoogde druk op het rioolsysteem. In 2100 zal deze trend zich voortzetten, mogelijk met nog intensere buien, waardoor wateroverlast in bebouwd gebied en tijdelijke overstromingen van kleine waterwegen en afwateringssystemen vaker zullen voorkomen. Seizoensgebonden verschillen zijn hierbij van belang: extreme neerslag zal vooral in de herfst en winter toenemen, wat ook een effect heeft op de frequentie en intensiteit van hoogwaterpieken in rivieren. Dit verhoogt het risico op dijkdoorbraken en overstromingen in rivierdelta's en laaggelegen delen van Nederland.

Naast structurele wateroverlast kunnen extreme situaties optreden, zoals langdurige regenperiodes die leiden tot vollopen van bekkens en kanalen, met risico's voor zowel de stedelijke als de landelijke omgeving waarin datacenters geplaatst zijn.

Klimaatdreiging(en) contextscenario 'sterk risicoverhogend'

In het sterk risicoverhogende scenario neemt de intensiteit van extreme neerslag en de stijging van de zeespiegel significant toe. De zeespiegelstijging in 2100 kan oplopen tot 1,2 meter, waardoor de waterveiligheid in kustgebieden ernstig onder druk komt te staan. Dit verhoogt de kans op stormvloed en dijkdoorbraken, vooral in de westelijke provincies en delen van Friesland en Groningen. In combinatie met een toename van piekafvoeren in rivieren ontstaat een aanzienlijk groter risico op overstromingen in de grote rivierendelta's.

Voor 2050 wordt al een sterke toename van extreme neerslag verwacht, met 5-9% intensere regenbuien en een grotere kans op hevige zomeronweer. Dit leidt tot wateroverlast in stedelijke gebieden, waar het huidige rioolstelsel onvoldoende capaciteit heeft om plotselinge grote hoeveelheden neerslag te verwerken. In 2100 nemen deze risico's verder toe, met mogelijk 26% zwaardere piekbuien in de zomer. De kans op dijkdoorbraken en overstromingen in poldergebieden neemt hierdoor aanzienlijk toe, vooral in situaties waarin hoge rivierafvoeren samenvallen met stormvloed langs de kust.

Geografisch gezien zijn vooral de Randstad, de grote rivierendelta's en de kustgebieden kwetsbaar voor deze ontwikkelingen.

In onderstaande tabel zijn de veranderingen uit KNMI'23 [8] weergegeven die voor datacenters (donker blauw) relevant zijn rondom natte dagen en neerslag:

			Klimaatscenario's: Ln=Beperkt, Hd=Sterk			
			2050		2100	
Klimaat	Bron	Huidig	Beperkt	Sterk	beperkt	Sterk
Jaarneerslag (mm)	KNMI'23	851	3%	-2%	3%	-3%
Zomerneerslag (mm)	KNMI'23	235	-2%	-13%	-2%	-29%
Zomers 1-daagse bui die eens in 10 jaar valt (mm) (intensiteit)	KNMI'23	63	+5%	+6%	+5%	+9%
Zomerse urneerslag die eens per jaar wordt overschreden (mm) (intensiteit)	KNMI'23	16	+6%	+6% (+11%)	+5%	+15% (+26%)

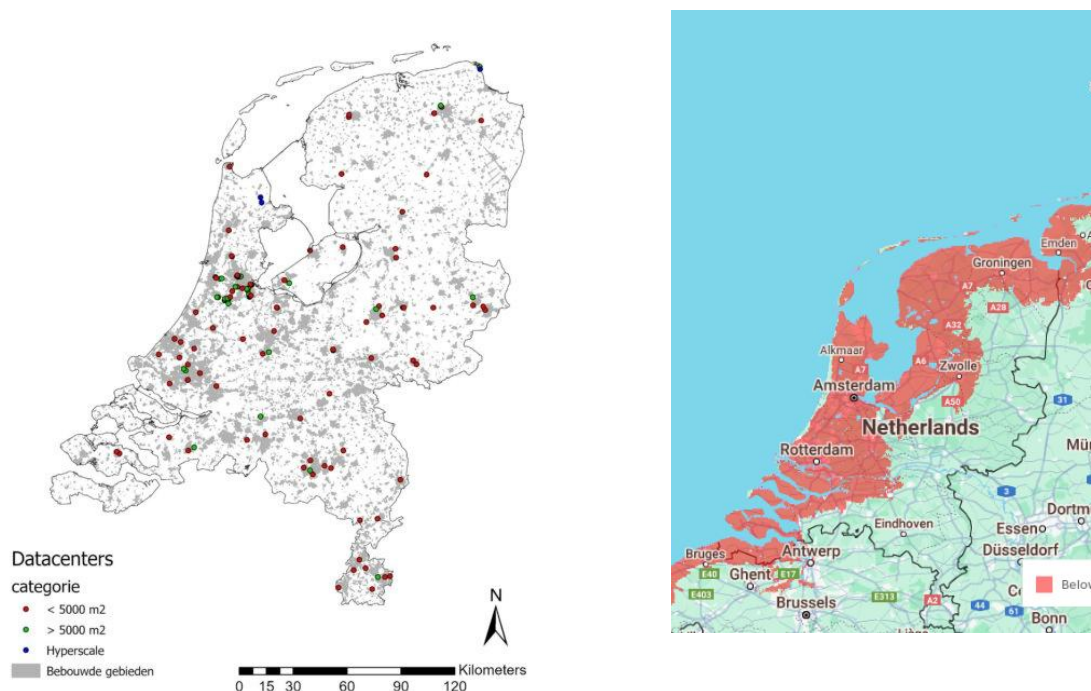
De totale jaarlijkse neerslag verandert beperkt, zowel het beperkte (Ln) scenario voor 2050 en 2100 (beide +3%) als in het sterke (Hd) scenario (-2% tot + 3%). De verdeling verandert sterk in het sterke scenario, de zomerneerslag neemt hier significant af (-13% tot -29%), wat de beschikbaarheid van koelwater uit natuurlijke bronnen kan beïnvloeden. Hevige regenbuien worden intenser: een extreme zomerse bui (eens in 10 jaar) wordt in een sterk scenario 6% in 2050 en 9% zwaarder in 2100. Urneerslagpieken (in mm) worden heftiger (+6% tot +15%), wat wateroverlast en overstromingsrisico's kan verhogen, ook rondom datacenters. Hevigere regenbuien en extreme neerslag kunnen leiden tot overstromingsrisico's, waardoor de locatiekeuze en lokale maatregelen tegen waterafvoer van datacenters belangrijker worden.

Zeespiegelstijging vormt een aanzienlijke bedreiging voor laaggelegen gebieden in Nederland, vooral in regio's onder zeeniveau en dicht bij de kust. In de KNMI '23 klimaatscenario's [8] projecties wordt rond 2050 in lage uitstootscenario's een stijging van 16 tot 34 cm verwacht, en in hoge uitstootscenario's een stijging van 19 tot 38 cm. Rond 2100 is dit bij lage uitstootscenario's een stijging van 26 tot 73 cm, en bij hoge uitstootscenario's een stijging van 59 tot 124 cm. In extreme gevallen, bij hoge uitstoot en versneld smelten van Antarctisch ijs, kan de zeespiegelstijging tegen 2100 zelfs oplopen tot 2,5 meter.

Figuur 14 toont de locaties van datacenters in Nederland, met oppervlakte <5000 m², >5000 m² en de twee hyperscale locaties in Eemshaven en Middenmeer. Deze kaart is door TNO gemaakt op basis van een lijst van 142 datacenter locaties op basis van informatie van Dutch Data Center Association [64], website van Baxtel en Google Maps. De datacenters liggen verspreid over Nederland, met de meeste datacenters in de regio MRA, en twee hyperscale locaties in Middenmeer, Noord-Holland en in Eemshaven, Groningen.

Diverse gebieden in Nederland lopen risico op overstromingen in 2050 en later, zoals blijkt uit wereldwijde studie van Climate Central [65]. In deze studie is ook een interactieve kaart beschikbaar met overstromingsrisico in de periode 2030 tot 2150. Deze kaart is gebaseerd op IPCC 2021 en keringen in verschillende landen wereldwijd. In de Randstad bevinden steden als Amsterdam, Rotterdam en Den Haag zich in laaggelegen gebieden en zijn kwetsbaar voor zowel zeespiegelstijging als verhoogde rivierafvoeren. Groningen en

omliggende gebieden in Noord-Nederland kunnen tegen 2050 regelmatig te maken krijgen met overstromingen die tot aan de Hondsrug reiken, zie Figuur 14 op basis van interactieve risicokaart van Climate Central [66]. Ook in de Zuidwestelijke delta zijn provincies Zeeland en delen van Zuid-Holland extra kwetsbaar vanwege hun ligging aan zee en de aanwezigheid van grote rivieren.



Figuur 14 Locaties van datacenters in Nederland(links) en delen van Nederland onder overstromingsniveau in 2100 bij een Hoog uitstootscenario (rechts).

Secundaire effecten

Er zijn geen secundaire effecten bekend voor overstromingen.

5.5.2 Adaptatiemaatregelen huidig beleid

Sinds 2022 is de richtlijn EU 2022/2557 betreffende de weerbaarheid van kritieke entiteiten van de Europese Unie van kracht (CER-richtlijn), welke van belang is voor de bescherming van datacenters voor overstromingen. In de richtlijn is ook weerbaarheid tegen natuurrampen opgenomen. De naleving hiervan is een wettelijke verplichting en geldt ook voor aanbieders van datacenterdiensten zoals gedefinieerd in artikel 6, punt 31, van richtlijn EU 2022/2555. Deze CER-richtlijn biedt richtlijnen voor het ontwerpen en bouwen van datacenters met inachtneming van mogelijke natuurrisico's. Zo bestaan er richtlijnen voor risicobeoordeling, ontwerp en beveiliging van datacenters met betrekking tot natuurrampen en andere bedreigingen. Dit kan onder andere betekenen dat datacenters strategisch worden geplaatst in gebieden met een lager risico op overstromingen en andere natuurrampen, of dat er specifieke bouwtechnieken worden toegepast, zoals verhoogde bouwlocaties, waterdichte compartimentering en robuuste noodstroomvoorzieningen.

Er is aandacht voor het overstromingsrisico van datacenters in huidig beleid, maar dit wordt vooral indirect meegenomen via bestaande waterveiligheidsnormen en toekomstige toetsingen. Adaptatiemaatregelen zoals klimaatadaptieve bouw en mogelijke aanpassing van waterveiligheidsnormen spelen hierbij een rol.

In de Datacenterstrategie 2025-2027 van Noord-Holland [67] zijn een aantal overwegingen opgenomen met betrekking tot waterveiligheid en wateroverlast voor datacenters. Datacenters bevinden zich in gebieden die worden beschermd door primaire (duinen en dijken rond het IJssel- en Markermeer) en regionale waterkeringen (kades langs kanalen, rivieren en boezems). De veiligheidsnormen van deze keringen zijn gebaseerd op economische waarde en mogelijke schade bij een overstroming. De vestiging van datacenters kan mogelijk leiden tot aanpassingen in deze normen en extra kosten voor bijvoorbeeld dijkversterkingen voor gebieden met datacenters door hun economische waarde.

Om extra schade te voorkomen kunnen datacenters klimaatadaptief gebouwd worden door ze op een terp te plaatsen [67] zodat ze bij overstromingen niet onder water komen te staan. De provincie Noord-Holland evalueert periodiek de waterveiligheidsnormen en kan besluiten om ze te verhogen op basis van nieuwe ontwikkelingen. In de daaropvolgende toetsronde wordt beoordeeld of extra maatregelen, zoals dijkversterking, nodig zijn en welke kosten dit met zich meebrengt.

Datacenters stellen hoge eisen aan beschikbaarheid, wat leidt tot uitgebreide redundantiemaatregelen die ook bijdragen aan klimaatadaptatie. Zo worden back-up locaties die bij uitval kunnen worden ingeschakeld vaak geselecteerd op basis van criteria die het risico op gelijktijdige uitval minimaliseren. Bij een back-up locatie wordt gelet op ligging buiten hetzelfde overstromingsgebied, bijvoorbeeld in een andere polder [interview Bytesnet].

Het overstromingsrisico bij datacenters kan aanzienlijk worden beperkt door strategische bouwmaatregelen. Een effectieve aanpak is het plaatsen van de datavloer en alle essentiële apparatuur op een verhoging, zodat deze beschermd blijven bij wateroverlast. Een goed voorbeeld hiervan is het Equinix-datacenter AM4 op het Science Park in Amsterdam, een datatoren van 72 m hoog met 12 verdiepingen [68]. Nog robuuster zijn de Alticom-datacenters, die zijn gevestigd in voormalige zendmasten van KPN. Het Alticom-datacenter in Wormerveer ligt bijvoorbeeld 0,7 m onder NAP, maar dankzij de verhoogde constructie vormt overstroming daar geen reëel risico. Een ander voorbeeld van hoe datacenters robuust gebouwd kunnen worden is van Equinix, met aangepaste ontwerpeisen voor nieuwe datacenters op basis van klimaatrisico's, zoals overstromingen [69]. Als de geplande locatie van een datacenter risico loopt op overstromingen door hevige regen, kan wordt het voorzien van een drainagesysteem. Dit voorkomt dat regenwater zich ophoopt en het gebouw omringt na een zware regenbui. Bij een risico op kustoverstromingen worden in het ontwerp barrières opgenomen om binnendringend zeewater tegen te houden.

5.5.3 Blootstelling

Blootstelling bij contextscenario 'beperkt risicoverhogend' en huidig beleid

Deltares heeft een studie gedaan naar de huidige watergerelateerde klimaatrisico's [70].

Deze is gebruikt in deze aanvullende analyse door TNO over risico's op de digitale infrastructuur, en specifiek voor overstromingsrisico's van datacenters. Verder is ook gebruikt gemaakt van de kaarten van de Klimateffectatlas Nederland met specifieke kaarten met

plaatsgebonden overstromingskansen, huidig en in 2050 en 2100, met verschillende hoogtes van 0, 20, 50 en 200 cm.

In het **beperkt risicoverhogende scenario (Ln)** neemt de zeespiegel toe met ongeveer 0,3 meter in 2050, en loopt dit op tot maximaal 0,73 meter in 2100. Vooral risicovol is dat de intensiteit van neerslag zal toenemen, met name in de wintermaanden. Piekafvoeren van grote rivieren zoals de Rijn en Maas zullen waarschijnlijk toenemen met zo'n 10 tot 20% [71]. In dit scenario blijft het overstromingsrisico in de meeste regio's beheersbaar onder het huidige beschermingsniveau van primaire en regionale waterkeringen. Echter, lokale wateroverlast in stedelijke gebieden (waar drainagecapaciteit vaak al onder druk staat) zal waarschijnlijk frequenter optreden. Omdat veel datacenters zich in verstedelijkt en laaggelegen gebied bevinden, zoals de Metropoolregio Amsterdam, Zuid-Holland en Flevoland, kan deze lokale wateroverlast operationele risico's opleveren.

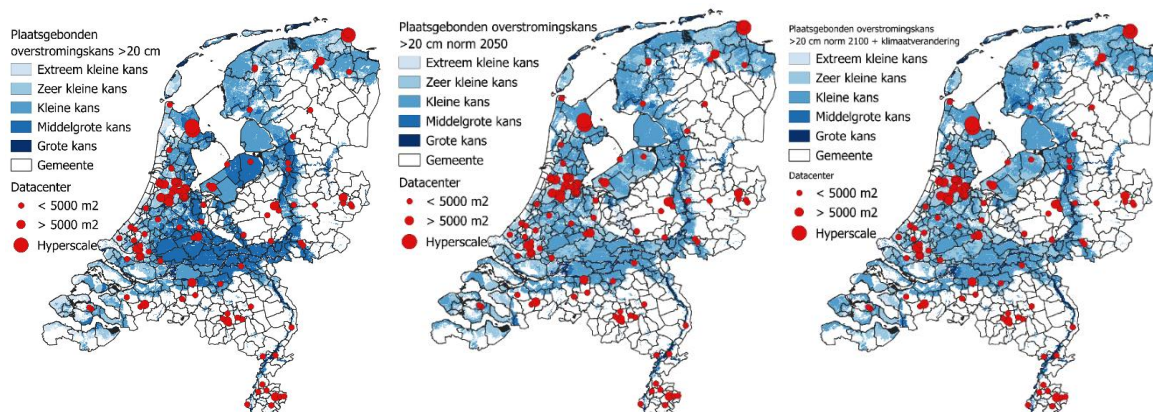
Blootstelling bij contextscenario 'sterk risicoverhogend' en huidig beleid

In het **sterk risicoverhogende scenario (Hd)** is sprake van een drastischer ontwikkeling. De zeespiegelstijging bedraagt in dit geval naar verwachting 0,45 meter in 2050 en loopt op tot tussen de 1,24 en 2,5 meter in 2100, afhankelijk van de mondiale uitstootontwikkeling en mogelijke instabiliteit van ijskappen. Bovendien nemen piekafvoeren van rivieren in dit scenario toe met 20 tot 40%, waardoor de kans op overstromingen aanzienlijk toeneemt. Ook langdurige droogte kan de stabiliteit van dijken aantasten, bijvoorbeeld door bodemdaling of verdroging van veenlagen, wat de veiligheid van waterkeringen ondermijnt. De dijken die echter het meest risico lopen zijn regionale, secundaire waterkeringen, die minder sterk zijn dan onze primaire waterkeringen langs de kust en de grote rivieren [72].

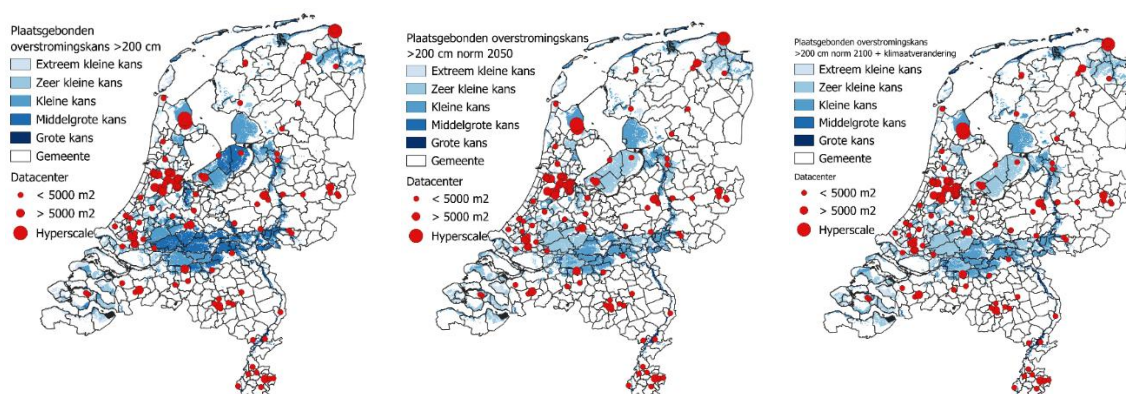
De datacenterlocaties, zoals weergegeven Figuur 15 en Figuur 16, laten zien dat een substantieel deel zich bevindt in laaggelegen polders, langs rivieren of nabij de kust. Denk hierbij aan clusters in de Randstad, waaronder Amsterdam, Haarlem, en Almere, maar ook aan regio's als het Rivierengebied, Brabant en Zuid-Hollandse delta. Deze ligging maakt ze in toenemende mate kwetsbaar voor zowel zeespiegel- als riviergebonden overstromingen, maar op de geïntegreerde overstromingskaarten is te zien dat vooral riviergebonden overstromingen een risico lijken te zijn.

TNO heeft een analyse gemaakt van de locaties van datacenters in Nederland en de overstromingskansen nu en in 2050 en 2100 op basis van de normen die dan gelden. Er is een adressenlijst met 142 datacenters gebruikt van Dutch Data Center Association, en de informatie van de Klimaat-effectatlas Nederland, die is gebaseerd op informatie van Landelijk Informatiesysteem Water en Overstromingen (LIWO).

In Figuur 15 en Figuur 16 is de plaatsgebonden overstromingskans >20 cm en >200 cm getoond, samen met de locaties van datacenters in Nederland.



Figuur 15 Plaatsgebonden overstromingskans >20 cm en locaties datacenters in Nederland; huidig (links), norm 2050 (midden) en norm 2100 (rechts) [TNO]



Figuur 16 Plaatsgebonden overstromingskans >200 cm en locaties datacenters in Nederland; huidig (links), norm 2050 (midden) en norm 2100 (rechts) [TNO]

In Tabel 2 is te zien hoeveel datacenters in de verschillende zones met een plaatsgebonden overstromingskans >20 cm liggen op basis van de huidige situatie en in 2050 en 2100. 45,1% van de datacenters (totaal: 142) ligt bijv. in gebieden met geen kans op een plaatsgebonden overstroming >20 cm, nu en in de toekomst. 11,3% ligt in nu een gebied met een middelgrote kans (eens per 30 tot 300 jaar) en dit percentage neemt af naar 0% in 2050 en 2,8% in 2100. In 2050 en 2100 neemt de plaatsgebonden overstromingskans >20 cm dus af voor de datacenters samen, door de hogere normen in 2050 en 2100 van primaire en secundaire waterkeringen in Nederland. Het risico op overstromingen neemt hiermee dus af in 2050 en 2100, en afhankelijk van de aanvullende maatregelen bij nieuwe datacenters zelf (bijv. apparatuur niet op begane grond) zal de impact van overstromingen verder worden verlaagd.

Tabel 2 Percentage datacenters met kans op plaatsgebonden overstroming >20 cm, in huidige situatie en in 2050 en 2100 (Bron: TNO)

Plaatsgebonden overstromingskans >20 cm; huidige situatie, 2050 en 2100				
Zone	Kans	Huidig	2050	2100
Geen kans	Nooit	45,1%	45,1%	45,1%
Extrem kleine kans	1/30.000 jaar	16,2%	10,6%	9,9%

Zeer kleine kans	1/3.000 tot 1/30.000 jaar	17,6%	28,2%	27,5%
Kleine kans	1/300 tot 1/3.000 jaar	9,9%	16,2%	14,8%
Middelgrote kans	1/30 tot 1/300 jaar	11,3%	0,0%	2,8%
Grote kans	>1/30 jaar	0,0%	0,0%	0,0%

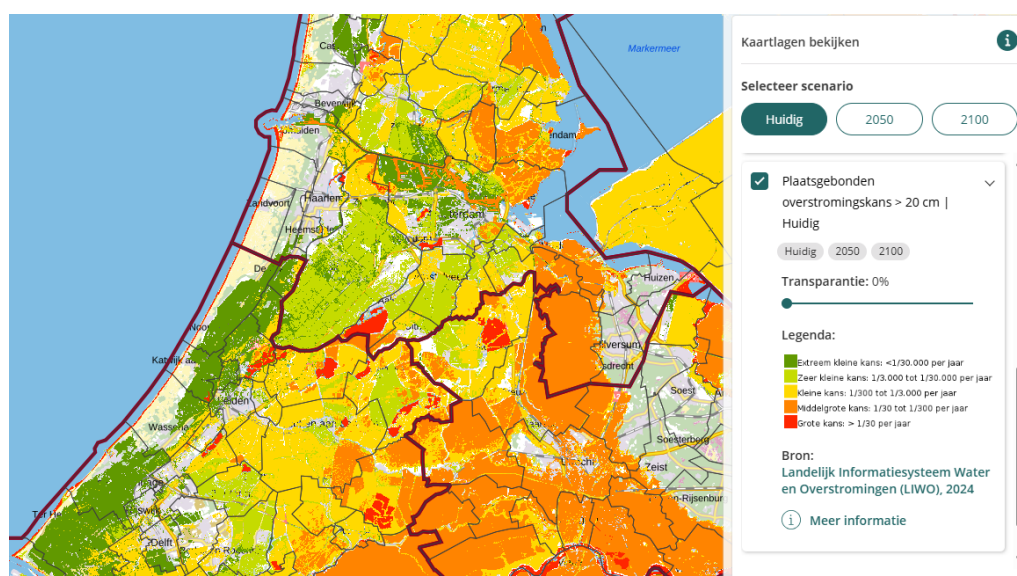
In Tabel 3 is een vergelijkbare analyse gedaan voor de kans op plaatsgebonden overstroming >200 cm, in huidige situatie en in 2050 en 2100. 86,6% van de 142 datacenters ligt in een gebied met geen kans op overstroming >200 cm. Ook hier neemt het risico op overstromingen >200 cm voor de 142 datacenters af in 2050 en 2100.

Tabel 3 Percentage datacenters met kans op plaatsgebonden overstroming >200 cm, in huidige situatie en in 2050 en 2100 (Bron: TNO)

Plaatsgebonden overstromingskans >200 cm; huidige situatie, 2050 en 2100				
Zone	Kans	Huidig	2050	2100
Geen kans	Nooit	86,6%	86,6%	86,6%
Extreem kleine kans	1/30.000 jaar	1,4%	2,1%	2,1%
Zeer kleine kans	1/3.000 tot 1/30.000 jaar	7,0%	8,5%	8,5%
Kleine kans	1/300 tot 1/3.000 jaar	2,1%	2,8%	2,8%
Middelgrote kans	1/30 tot 1/300 jaar	2,8%	0,0%	0,0%
Grote kans	>1/30 jaar	0,0%	0,0%	0,0%

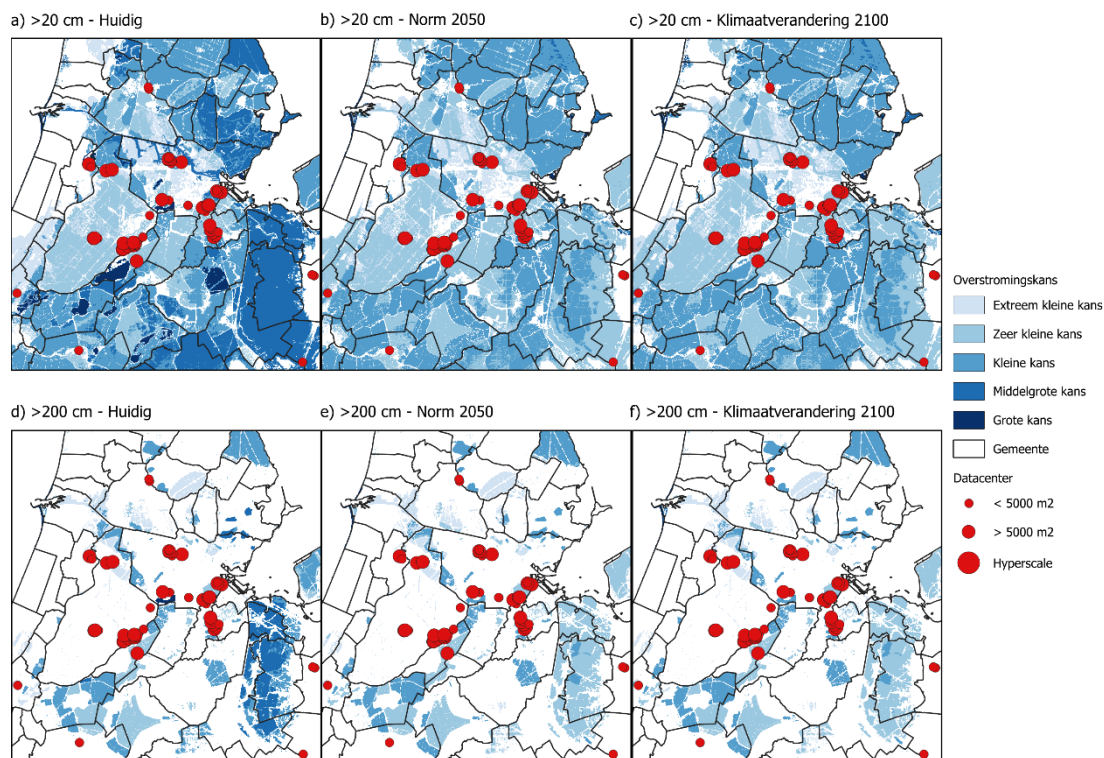
Metropoolregio Amsterdam en hyperscale datacenters

Voor de Metropoolregio Amsterdam (MRA) en de twee aangewezen locaties voor hyperscale datacenters is in een aanvullende analyse uitgevoerd. In Figuur 17 is de plaatsgebonden overstromingskans >20 cm getoond voor de regio Amsterdam op basis van een interactieve kaart van de Klimaateffectatlas [30]. Hierin is te zien dat het merendeel van het gebied een kleine (geel) of zeer kleine (lichtgroen) kans op overstromingen heeft. De risico's voor datacenters in dit gebied zijn dus klein, ondanks dat een groot deel van dit gebied enkele meters onder NAP ligt.



Figuur 17 Plaatsgebonden overstromingskans >20 cm in huidige situatie (Bron: Kaartviewer op Klimaateffectatlas [30])

In Figuur 18 zijn de datacenters in de MRA geplot op de kaarten met een plaatsgebonden overstromingskans >20 cm en >200 cm. De datacenters liggen verspreid in en rondom Amsterdam, met veelal een kleine tot zeer kleine kans op overstromingen.



Figuur 18 Plaatsgebonden overstromingskans >20 cm voor MRA in huidige situatie, 2050 en 2100 (a-c) en Plaatsgebonden overstromingskans >200 cm in huidige situatie, 2050 en 2100 (d-f).

5.5.4 Gevoeligheid

Datacenters moeten zowel fysiek als digitaal veilig zijn, wat samenwerking tussen bedrijven en overheden vereist. De clustering van datacenters kan in theorie een kwetsbaarheid vormen, waardoor bedrijven steeds vaker werken met replicatie en back-upsystemen. Een intelligente back-upstrategie kan helpen om storingen op te vangen en de veerkracht van de sector te vergroten. Steeds meer bedrijven kiezen ervoor om hun dataverkeer uit te besteden, maar willen essentiële bedrijfsdata en IT dichtbij houden, binnen een maximale reistijd van 30 minuten. Om de veerkracht van de datacentersector te vergroten, wordt in Zuid-Holland een back-upstrategie ontwikkeld [73]. Daar is een sterke energie-infrastructuur en goede aansluiting op digitale netwerken en warmtenetwerken. Voor bedrijven met minder strenge latency-eisen kan een grotere afstand tot internetknooppunten zoals AMS-IX acceptabel zijn. Regio's zoals Zuid-Holland, Middenmeer en de oostflank van Utrecht worden daarom overwogen als mogelijke (back-up) locaties voor toekomstige datacenters. Het zou denkbaar zijn om back-up locaties in de verdere toekomst (2050-2100) nog verder weg te zetten, gezien het overstromingsrisico van een aanzienlijk deel van Nederland. Hyperscalers maken voor hun cloudiensten al gebruik van meerdere datacenters verspreid over Europa (met name Noordwest Europa) en back-up via datacenters in andere regio's (zoals VS, Azië).

Ook het Deltaprogramma [70] benoemt specifiek de kwetsbaarheid van economische functies in deze regio's, waaronder digitale infrastructuur: denk aan bedrijfsuitval en schade die samenhangt met uitval van infrastructuur en nutsdiensten, maar ook langetermijnpact op het investeringsklimaat.

5.5.5 Impact

De impact van een overstrooming op een datacenter heeft vooral te maken met veroorzaakte keteneffecten die verder reiken dan de fysieke locatie zelf. Datacenters vormen de ruggengraat van onze digitale infrastructuur: ze huisvesten servers voor cloudopslag, applicaties, websites, overheidsdiensten en bedrijfsnetwerken, en verzorgen daarnaast belangrijke connectiviteit via internetknooppunten.

Wanneer een datacenter overstroomt, valt doorgaans eerst de elektriciteit uit. Dit gebeurt ofwel direct, door ondergelopen infrastructuur, ofwel preventief, door uitschakeling van het netwerk om kortsluiting of elektrocutie te voorkomen. Hoewel veel datacenters over noodstroomvoorzieningen (zoals dieselgeneratoren en UPS-systemen) beschikken, zijn deze slechts bedoeld voor tijdelijke overbrugging. Als de overstrooming aanhoudt, kan ook deze redundantie uitvallen. Bovendien kunnen bij extreme situaties ook de toegangswegen, onderhoudsnetwerken of koelvoorzieningen worden geraakt, waardoor de operationele continuïteit alsnog in gevaar komt.

Een uitval van stroom en connectiviteit in een datacenter heeft ook bredere maatschappelijke gevolgen. In het getroffen gebied kan dit leiden tot uitval van:

- ☐ **Telecommunicatie en mobiele netwerken**, indien centrale netwerkapparatuur in het datacenter is ondergebracht.
- ☐ **Internettoegang**, met name bij colocatie- of interconnectiepunten.
- ☐ **Vitale diensten** zoals betalingsverkeer, overheidsportalen, logistieke systemen, zorginformatiesystemen of industriële processen.

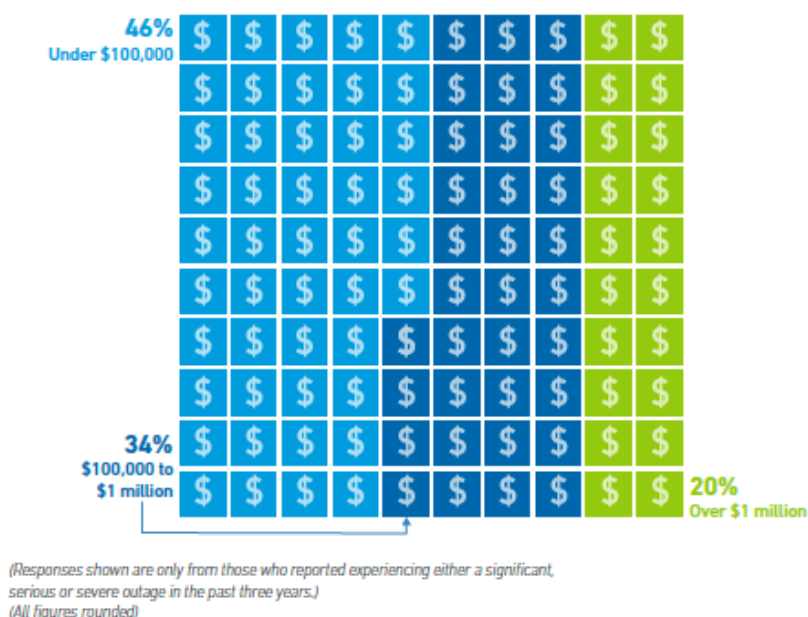
De ernst van de impact hangt af van de duur van de uitval. Korte onderbrekingen (enkele minuten tot uren) zijn vaak overbrugbaar door back-ups en failover-systemen naar andere datacenters. Wel kunnen gebruikers hinder ondervinden, en kan dataverlies optreden als replicatie vertraagd is. Langdurige uitval (dagen of langer) kan leiden tot blijvende dataverlies, reputatieschade voor bedrijven, economische verstoringen en bij uitval van ICT voor zorg- of hulpdiensten zelfs tot risico's voor de volksgezondheid en veiligheid.

Ordeschatting van financiële kosten van digitale verstoringen

In "Annual outage analysis 2025" [38] is data geanalyseerd om een beeld te krijgen van oorzaken, frequentie en consequenties van uitval van ICT en datacenters. Om een inschatting te maken van de economische impact van digitale verstoringen, en in het bijzonder verstoringen in datacenters, is gebruikgemaakt van gegevens uit dit rapport [38]. Hoewel klimaatrisico's in dit rapport niet expliciet worden benoemd (omdat de analyse zich richt op het *type* verstoring in plaats van de onderliggende *oorzaak*), biedt het rapport wel nuttige cijfers over het aantal incidenten, hun frequentie en de directe economische schade per incident.

Voor Nederland zijn de volgende aannames gedaan:

- **Aantal datacenteraanbieders:** Nederland telt circa 100 datacenteraanbieders (Dutch Data Center Association, 2024).
- **Frequentie van grote verstoringen:** Volgens het rapport [38] van Uptime Institute heeft 9% van de respondenten in de afgelopen drie jaar een ernstige verstoring ervaren. Dat komt neer op gemiddeld 3% per jaar.
- **Kosten per ernstige verstoring:** Uit de analyse blijkt dat de directe kosten per ernstige storing variëren van minder dan \$100.000 (46%) tot meer dan \$1 miljoen (20%), zie Figuur 19. Een conservatieve schatting op basis van deze gegevens van de gemiddelde kosten per incident is ongeveer €600.000.



Figuur 19 Financiële impact van ernstige datacenterstoringen (Bron: Uptime Institute [38]).

Op basis hiervan ontstaat de volgende grove ordeschatting voor Nederland:

Totale jaarlijkse directe kosten: 100 colocatie datacenters × 3% kans op ernstige storing × €600.000 = €1,8 miljoen per jaar aan directe schade.

Wat betreft de relatie met klimaatrisico's: hoewel het exacte aandeel van klimaatgerelateerde storingen moeilijk is vast te stellen, kan op basis van expertinschatting een bovengrens van 10% worden aangenomen. Dat zou betekenen dat circa €180.000 per jaar aan schade direct of indirect terug te voeren is op klimaatgerelateerde verstoringen. Binnen het schaal kader van het PBL is dit een zeer lage schadepost, die bovendien voor rekening komt van de private sector.

De indirecte effecten van ICT-verstoringen zijn en worden dus potentieel aanzienlijk groter, vooral gezien de verwevenheid van digitale infrastructuur met vitale maatschappelijke processen. Volgens een rapport van Deloitte [74] kan een tijdelijke internetonderbreking in een land met hoge connectiviteit een geschatte impact hebben van ongeveer \$23,6 miljoen

per 10 miljoen inwoners per dag, wat neerkomt op ongeveer 1,9% van het dagelijkse BBP. Forbes [75] stelt dat de kosten van downtime voor grote organisaties gemiddeld \$9.000 per minuut bedragen, wat neerkomt op \$540.000 per uur. Het ITIC 2024-rapport [76] constateert dat voor 90% van de bedrijven de kosten van een uur downtime meer dan \$300.000 bedragen, waarbij 41% aangeeft dat deze kosten kunnen oplopen tot tussen \$1 miljoen en \$5 miljoen per uur. Een onderzoek uitgevoerd door Infonetics Research [77] toonde aan dat bedrijven gemiddeld bijna \$4 miljoen per jaar verliezen door ICT-uitval, wat ongeveer 0,5% van hun totale omzet vertegenwoordigt. Hierbij dient te worden opgemerkt dat ICT-verstoringen slechts in een (zeer) klein deel worden veroorzaakt door de klimaatrisico's.

Ter illustratie: bij de recente landelijke stroomuitval in Spanje werden de economische kosten geschat op €400 miljoen [78]. Dit betrof weliswaar de gehele economie, maar het laat zien dat stroomuitval verstrekende keteneffecten kan hebben, ook als sommige datacenters blijven functioneren op noodstroom of via back-up locaties. Hoewel redundantie en back-upsystemen de directe impact van storingen beperken, blijft de afhankelijkheid van stroom- en netwerkcontinuïteit een aandachtspunt binnen de bredere context van klimaatadaptatie en risicobeheersing van digitale infrastructuur.

De toenemende kritieke aard van digitale diensten zal deze kosten in de toekomst waarschijnlijk verder opdrijven, waarbij sommige incidenten een domino-effect hebben op veel klanten en hun diensten. Het meest prominente voorbeeld hiervan is de CrowdStrike-storing op 19 juli 2024, die naar schatting een wereldwijde financiële impact van \$10 miljard heeft gehad. Deze verstoringen werden veroorzaakt door een foutieve patch op Microsoft Windows van de beveiligingssoftware van externe partij CrowdStrike. Verder is er de recente grote storing bij AWS op 20 oktober 2025 die impact heeft gehad op veel verschillende diensten wereldwijd.

De stijgende verwachtingen van klanten, bedrijven en toezichthouders worden weerspiegeld in strengere Service Level Agreements (SLA) en, in sommige gevallen, boetes van toezichthouders. Deze financiële druk versterkt de businesscase voor blijvende beschikbaarheid van ICT en clouddiensten en investeringen in weerbaarheid.

5.6 Klimaatrisicoanalyse voor digitale infrastructuur als geheel

In deze paragraaf zijn de individuele klimaatrisicoanalyse voor de verschillende dreigingen en onderdelen uit paragraaf 5.2 t/m 5.5 samengevoegd om de eindimpact op de digitale infrastructuur als geheel te bepalen.

In het onderzoek naar de klimaatrisico's is gebruik gemaakt van de PBL-scenario's:

- ☐ Beperkt risicoverhogend (Ln, 2050 & 2100): lage klimaatverandering en relatief natte omstandigheden.
- ☐ Sterk risicoverhogend (Hd, 2050 & 2100): hoge klimaatverandering en langdurige droge periodes.

In de analyse is met name gekeken naar de scenario's in 2050. Door de snelle ontwikkelingen in de digitale sector en de bijbehorende korte vervangingscycli van apparatuur in netwerken en datacenters (typisch <10 jaar) is de verwachting dat er voldoende

adaptatie mogelijk is voor klimaatrisico's op de langere termijn tot 2100. Alleen voor het klimaatrisico overstromingen is 2100 relevant, omdat keuzes voor nieuwe, fysieke locaties (lees gebouwen, stroomvoorziening, glasvezelinfrastructuur) voor bijvoorbeeld hyperscale datacenters of uitbreidingen van infrastructuur in de regio MRA met hyperconnectiviteit op lange termijn van belang zijn.

5.6.1 Klimaatdreigingen met risico op verstoringen in de fysieke infrastructuur

Het grootste klimaatrisico voor de digitale infrastructuur is een secundair effect door grootschalige uitval van stroomvoorziening door het optreden van klimaatrisico's. Voor (hyperscale) datacenters en centrale netwerkklocaties worden back-up voorzieningen (UPS) gebruikt die meerdere dagen kunnen blijven werken. Echter, richting de 'randen' van de netwerken en voor de internet- en netwerkaansluitingen voor bedrijven en consumenten is er geen back-up of zeer beperkte back-up van 2-3 uur (bijvoorbeeld in mobiele masten) vanuit het netwerk. Hierdoor zal een groot deel van de bedrijven en consumenten geen gebruik meer kunnen maken van ICT en internet, tenzij men zelf lokale back-up voorzieningen heeft. Hieronder zijn de belangrijkste klimaatdreigingen met primaire impact voor de digitale sector beschreven:

1. **Periode van extreme hitte:** extreme hitte kan voor een tijdelijke piek in storingen van actieve apparatuur en/of koelsystemen zorgen. Datacenters moeten (gedeeltelijk) afschakelen door uitval van overbelaste koelsystemen of door onvoldoende koelcapaciteit bij langere periode van extreme hitte. Netwerkapparatuur in masten en straatkasten kan ook te warm worden, waardoor de kans op verstoringen toeneemt, of moet worden afgeschakeld. Apparatuur werkt in het algemeen ook bij extreme temperaturen (-20 tot +50 graden), de kans op verstoringen neemt wel toe als apparatuur te warm wordt en moet worden uitgeschakeld. Een secundair effect is een (sterke) tijdelijke toename in stroomverbruik en (drink)watergebruik voor koeling van datacenters en andere technische ruimtes bij temperaturen boven 25-30 graden.
2. **Droogte met als secundair effect restricties op drinkwatergebruik:** Bij een lange periode van droogte kunnen problemen ontstaan met drinkwater en kan de overheid besluiten om restricties op drinkwatergebruik voor laagwaardig gebruik, zoals koeling van datacenters, op te leggen. Dit heeft gevolgen voor datacenters die gebruik maken van drinkwater voor koeling (ca 80% in 2024) en geen noodplan hebben om dit tekort aan te vullen met alternatieve bronnen. Bodemdaling vormt momenteel geen risico voor bijv. glasvezelkabels, deze zijn aangelegd in beschermende buizen, om kabelbreuk bij (lokale) verzakkingen te voorkomen.
3. **Neerslag en lokale overstroming door extreme neerslag:** bij extreme neerslag kan schade aan hardware in technische ruimtes ontstaan als deze onderlopen bij extreme, lokale neerslag met 20-50 cm. Daarnaast kan condens ontstaan in ruimtes of apparatuur, ook als temperatuur in een technische ruimte onder de 10 graden komt, dit geeft meer storingen en een kortere levensduur. Apparatuur in de directe buitenlucht is veelal goed beschermd tegen water van buiten, en ook wordt apparatuur in ruimtes beschermd door deze op hoogte te plaatsen (bijv. boven in kasten tussen 0,5 en 2 m). Overstroming van een groter gebied door piekafvoer van rivieren (zoals in Valkenburg) zorgt dat de stroomvoorziening preventief wordt afgeschakeld om risico op ongevallen door kortsluiting (en beschadiging van apparatuur) te voorkomen. Dit heeft directe impact op ICT-apparatuur in bijv. masten en straatkasten, aangezien

noodstroomvoorzieningen voor een beperkte periode van typisch 2-3 uur werkzaam zijn.

4. **Extreem weer (storm, windstoten, hagel, sneeuw, ijzel, onweer):** extreem weer, met name zware storm en windstoten, kan incidenteel leiden tot schade aan hardware dat buiten staat, bijv. aan antennes in masten of straatkasten. Risico's van blikseminslag zijn relatief klein, apparatuur kan goed worden beschermd door bliksemafleiders en goede aarding.
5. **Zeespiegelstijging:** de zeespiegelstijging leidt tot een verhoogde kans op overstromingen van delen van Nederland bij de huidige primaire en secundaire waterkeringen. Aanpassingen van de waterkeringen tot 2050 en 2100 zullen zorgen dat deze risico's niet groter maar kleiner worden. Bij de

5.6.2 Blootstelling, gevoeligheid, waarschijnlijkheid

Extreme hitte

- **Blootstelling:** landelijk met regionale verschillen binnen Nederland; datacenters, masten en straatkasten. Het aantal tropische dagen varieert sterk over Nederland, met gemiddeld 12 dagen in Nederland in het scenario sterk risicoverhogend' in 2050, maar minder dan 5 tropische dagen in het noordwesten en meer dan 20 in het zuiden (Zuidoost Brabant, Limburg). Binnen Europa is de blootstelling aanzienlijk hoger in Zuid- en Oost-Europa.
- **Gevoeligheid:** laag. Datacenters zijn ontworpen met voldoende koelcapaciteit, door adaptatie van koeling en apparatuur zal de gevoeligheid in de periode tot 2050 verder worden verlaagd. Ook voor masten en straatkasten is de gevoeligheid laag, gezien het feit dat in landen met extreme hitte mobiele en vaste netwerken ook voldoende betrouwbaar zijn.
- **Waarschijnlijkheid:** 1-10 jaar; Uitval t.g.v. klimaatrisico's wordt geschat op eens per 1 tot 10 jaar. Door de redundantie binnen ICT-netwerken en diensten blijft het maatschappelijk effect echter zeer klein. De directe kosten voor ernstige verstoring van een datacenter zijn 100 kEUR tot 1 MEUR, in het merendeel veroorzaakt door problemen met stroomvoorziening of koeling. Klimaatrisico's zijn hierbij niet de belangrijkste oorzaak, er zijn enkel incidentele voorbeelden door uitval bij extreme hitte.

Droogte met als secundair effect restricties op drinkwatergebruik

- **Blootstelling:** regionaal, datacenters. Bij restricties op drinkwatergebruik is de aanname dat restricties regionaal zullen zijn, dus per drinkwaterbedrijf (10 drinkwaterbedrijven in Nederland). Hiermee is de blootstelling op dit risico voor datacenters regionaal.
- **Gevoeligheid:** laag. Datacenters die drinkwater gebruiken hebben voldoende tijd om noodmaatregelen te nemen om watervoorraden tijdig aan te vullen. De hyperscale datacenters worden niet geraakt door restricties door het gebruik van regenwater of oppervlaktewater.
- **Waarschijnlijkheid:** 10-100 jaar; risico treedt pas op als secundair effect als er restricties komen op watergebruik door overheid. Dit is in Nederland nog niet gebeurd. De overheid kan verder ook uitzondering maken op mogelijke restricties voor watergebruik voor koeling binnen vitale infrastructuur zoals grotere datacenters (op basis van vermogen) en hoofdlocaties van telecomnetwerken.

Neerslag en lokale overstroming door extreme neerslag

- **Blootstelling:** landelijk met lokale verstoringen; datacenters, masten, straatkasten.
- **Gevoeligheid:** laag. Datacenters nemen reeds maatregelen tegen extreme neerslag, bijv. met lokale opvang, verbeterde afvoer of verhogingen. Het merendeel van de straatkasten en masten kan worden aangepast tegen lokale overstromingen van 20-50 cm. Echter, een

deel van deze locaties zal een hogere gevoeligheid hebben door hun ligging, met groter risico op lokale uitval.

- **Waarschijnlijkheid:** 1-10 jaar. Lokale verstoringen masten, straatkasten met beperkte impact.

Zeespiegelstijging en overstroming door rivieren

- **Blootstelling:** regionaal; datacenters, masten, straatkasten. Het risico op overstromingen in 20250 en 2100 door rivieren en zeespiegelstijging is in groot detail in kaart gebracht. Datacenters in zuiden en het oosten van Nederland liggen in gebieden die niet overstroomd worden. In het westen en noorden zijn er verschillen tot op lokaal niveau.
- **Gevoeligheid:** hoog. Bij een overstroming zal de stroomvoorziening worden uitgeschakeld of apparatuur in masten en straatkasten op afstand preventief worden uitgeschakeld. operationeel. Herstel is vaak niet direct mogelijk, doordat toegang in een overstroomd gebied langere tijd niet
- **Waarschijnlijkheid:** 10-100 jaar. ICT-voorzieningen worden met name geraakt door de uitval van de stroomvoorziening in overstroomd gebied als secundair effect. De impact is groter naarmate het overstroomd gebied groter is en meer masten/straatkasten worden geraakt.

5.6.3 Adaptatiemaatregelen op basis van huidig beleid

In de analyse naar adaptatiecapaciteit voor de verschillende klimaatrisico's - nu en in 2050/2100 – is gekeken naar mogelijkheden voor adaptatiemaatregelen vanuit de sector zelf en vanuit de overheid, zowel preventief om risico te verminderen als reactief om impact bij optreden te beperken. De digitale sector is een private sector, waarbij financiële afwegingen (op korte tot middellange termijn) bij individuele, commerciële aanbieders een belangrijke rol spelen, ook ten aanzien van klimaatrisico's en maatregelen. De overheid richt zich met beleid op het verkleinen van de blootstelling aan, gevoeligheid voor of impact van risico's op de middellange tot lange termijn.

In het algemeen geldt dat de impact van verstoringen, ook ten gevolge van klimaatrisico's, sterk kan worden verminderd door gebruik te maken van een hoge mate van redundantie in ICT-infrastructuur of van diensten. Voor vitale aanbieders is dit essentieel waardoor impact van de meeste klimaatrisico's verwaarloosbaar is en wordt beperkt door lokale, beperkte korte verstoringen. Individuele organisaties zijn zelf verantwoordelijk om weerbaar te zijn tegen uitval van ICT. Bijvoorbeeld door meerdere geografische verspreide datacenters te gebruiken (back-up, via 'twinning') of via clouddiensten met hoge beschikbaarheid. De overheid, inclusief Defensie, maakt ook gebruik van meerdere datacenters binnen Nederland.

Vanuit de overheid is er géén specifiek beleid dat direct gericht is op het verkleinen van klimaatrisico's voor de digitale sector (datacenters, netwerken, etc.). Wel is er indirect beleid en wetgeving, op twee gebieden: a) duurzaamheid en b) vitale infrastructuur. De digitale sector maakt 100% gebruik van elektriciteit voor de ICT-infrastructuur, waarmee 100% duurzaam energie uit zon of wind gebruikt kan worden. Voor aangewezen aanbieders van vitale ICT infrastructuur worden maatregelen gevraagd t.a.v. continuïteit, in de telecomwet (hoofdstuk 11a, artikel 11a.1 lid 2) en de Wwke voor vitale aanbieders. Hierin zijn generieke eisen opgenomen t.a.v. continuïteit, niet specifiek gericht op maatregelen tegen klimaatrisico's. Voor hyperscalers is er specifieke landelijke wetgeving die het voor gemeenten onmogelijk maakt om nieuwe locaties aan te wijzen voor hyperscale datacenters, gezien de impact op stroomvoorzieningen en stroomverbruik.

Extreme hitte – adaptatiecapaciteit en -maatregelen

- **Adaptatiecapaciteit vanuit de digitale sector:** vanuit duurzaamheid zijn er vanuit de sector verschillende initiatieven om o.a. het energieverbruik van datacenters te verminderen. Dit is voor een belangrijk deels ingegeven door verscherpte wetgeving op duurzaamheid, deels door kostenbesparing door lager energieverbruik o.a. voor koeling. Adaptatie vindt plaats door verbeterde apparatuur die typisch iedere 5-10 jaar wordt vervangen, door efficiëntere apparatuur/chips die minder warmte produceert, bij hogere temperaturen kan werken of andere koeltechnieken zoals *liquid cooling* gebruikt. Technische locaties, zowel bestaand als nieuw, worden aangepast aan veranderingen in het klimaat, bv. door meer koelcapaciteit of gesloten koelsystemen. Energieverbruik neemt wel toe als meer externe koeling nodig is. Voor masten en straatkasten vindt ook adaptatie plaats zoals betere monitoring van temperatuur en technische ruimte en van apparatuur, verbeterde, kleinere apparatuur die in masten geplaatst kan worden.
- **Adaptatie vanuit de overheid – huidig beleid:** Vanuit de overheid is er géén specifiek beleid dat direct gericht is op het verkleinen van klimaatrisico's voor datacenters. Nationale en Europese wetgeving vanuit duurzaamheid leidt tot investeringen in datacenters voor energie- en koelsystemen, die de klimaatrisico's van hitte en droogte verkleinen. Denk hierbij aan innovaties in koelsystemen, die minder of niet afhankelijk zijn van waterkoeling, bijv. waterkoeling vanaf hogere buitentemperaturen, *liquid cooling*, of waterkoeling via gesloten systemen of via opgevangen regenwater. Hierdoor worden datacenters minder afhankelijk van (drink)water of oppervlaktewater en het risico op (drink)waterrestricties bij periodes van droogte. Wetgeving vanuit duurzaamheid en ruimtelijke ordening kan ook leiden tot het verplaatsen van datacenters uit Nederland naar meer noordelijke landen. Omgekeerd kan Nederland aantrekkelijker worden als vestigingslocatie ten opzichte van Zuid-Europese landen.
- **(On)mogelijkheden voor adaptatie:** geen.

Droogte met als secundair effect restricties op drinkwatergebruik - adaptatiecapaciteit en -maatregelen

- **Adaptatiecapaciteit vanuit de digitale sector:** Datacenters in Nederland verbruiken relatief weinig drinkwater op jaarbasis: 0,089% van totaal in Nederland en 0,3% van zakelijke gebruik [37]. Vanuit de sector zijn er verschillende initiatieven om waterverbruik van datacenters te verminderen (met limiet van 0,4 l per KWh door CNDPCP). Andere maatregelen zijn gericht op verbeterde oplossingen voor koeling die minder of zelfs geen gebruik maken van drinkwater. Denk hierbij aan gesloten koelsystemen, opslag en gebruik van regenwater of oppervlaktewater (zie voorbeelden hyperscale datacenters Google en Microsoft in Nederland), en alternatieve koeltechnologie (zoals *liquid cooling*). De datacenters 'produceren' in bovenstaande voorbeelden meer water dan ze daadwerkelijk gebruiken en worden zo uiteindelijk 'water-positief'.
- **Adaptatie vanuit de overheid – huidig beleid:** wetgeving watergebruik datacenters, restricties op watergebruik bij schaarste. Verder waren drinkwaterbedrijven niet bereid om drinkwater voor koeling te leveren aan huidige en nieuwe hyperscale datacenters.
- **(On)mogelijkheden voor adaptatie:** het gebruik van drinkwater voor koeling is laag (0,1% op jaarbasis), met lokale verschillen en meer vraag op piekmomenten. Het gebruik van drinkwater voor koeling door datacenters is nog steeds hoog (79% in 2024), een afname in de komende jaren is niet voorzien, maar ook geen toename [50]. Om over te stappen naar alternatieve waterbronnen zoals regenwater of oppervlaktewater voor koeling is schaalgrootte nodig om de investeringen te rechtvaardigen. Voor hyperscale datacenters is dit nu het geval. De huidige 'waterpositieve' oplossingen voor de hyperscale datacenters zouden ook gerealiseerd kunnen worden voor hubs/clusters van

datacenters of andere grootgebruikers van koelwater. Dit vergt lokale afstemming tussen meerdere partijen, zoals leverancier industrieel/gefilterd water uit oppervlaktewater, of waterbedrijven (industrieel water), primaire afnemers koelwater (datacenters, industrie), secundaire afnemers water (bijv. tuinbouw/landbouw) en de overheid i.v.m. vergunningen.

Neerslag en lokale overstroming door extreme neerslag – adaptatiecapaciteit en -maatregelen

- ☐ **Adaptatiecapaciteit vanuit de digitale sector:** vanuit de sector worden verschillende maatregelen genomen tegen lokale overstroming door extreme neerslag. Bestaande technische gebouwen kunnen worden aangepast, bouweisen voor nieuwe locaties worden aangepast, en bij selectie van locaties kan men laag gelegen locaties vermijden. Ook kan apparatuur verhoogd worden geplaatst, bijv. hoger in een mast, of hoger in een straatkast.
- ☐ **Adaptatie vanuit de overheid – huidig beleid:** er is geen specifiek beleid en wetgeving op dit klimaatrisico.
- ☐ **(On)mogelijkheden voor adaptatie:** geen.

Zeespiegelstijging en overstroming door rivieren – adaptatiecapaciteit en -maatregelen

- ☐ **Adaptatiecapaciteit vanuit de digitale sector:** Datacenters stellen hoge eisen aan beschikbaarheid, wat leidt tot uitgebreide redundantiemaatregelen die ook bijdragen aan klimaatadaptatie. Zo worden back-up locaties geselecteerd op basis van criteria die het risico op gelijktijdige uitval minimaliseren. Bij een back-up locatie wordt gelet op ligging buiten hetzelfde overstromingsgebied of in een gebied zonder overstromingsrisico. Het overstromingsrisico bij datacenters kan aanzienlijk worden beperkt door strategische bouwmaatregelen. Een effectieve aanpak is het plaatsen van de datavloer en alle essentiële apparatuur op een verhoging, zodat deze beschermd blijven bij wateroverlast. Een goed voorbeeld hiervan is het Equinix-datacenter op het Science Park in Amsterdam, dat volledig op palen is gebouwd. Andere bouwmaatregelen zijn locaties voorzien van een drainagesysteem tegen extreme regenval of lokale opvang van regenwater in een lager gelegen bassin.
- ☐ **Adaptatie vanuit de overheid – huidig beleid:** sinds 2024 is de CER-richtlijn van de Europese Unie van kracht, welke van belang is voor de bescherming van datacenters voor overstromingen. Deze wetgeving biedt richtlijnen voor het ontwerpen en bouwen van datacenters met inachtneming van mogelijke natuurrisico's. Zo bestaan er richtlijnen voor risicobeoordeling, ontwerp en beveiliging van datacenters met betrekking tot natuurrampen en andere bedreigingen. Dit kan onder andere betekenen dat datacenters strategisch worden geplaatst in gebieden met een lager risico op overstromingen en andere natuurrampen, of dat er specifieke bouwtechnieken worden toegepast, zoals verhoogde bouwlocaties, waterdichte compartimentering en robuuste noodstroomvoorzieningen. Er is aandacht voor het overstromingsrisico van datacenters in huidig beleid, maar dit wordt vooral indirect meegenomen via bestaande waterveiligheidsnormen en toekomstige toetsingen. Adaptatiemaatregelen zoals klimaatadaptieve bouw en mogelijke aanpassing van waterveiligheidsnormen spelen hierbij een rol. In de Datacenterstrategie van Noord-Holland zijn een aantal overwegingen zijn opgenomen met betrekking tot waterveiligheid en wateroverlast voor datacenters. Datacenters bevinden zich in gebieden die worden beschermd door primaire (duinen en dijken rond het IJssel- en Markermeer) en regionale waterkeringen (kades langs kanalen, rivieren en boezems). De veiligheidsnormen van deze keringen zijn gebaseerd op economische waarde en mogelijke schade bij een overstroming. De vestiging van datacenters zorgen voor een hogere economische waarde en dit kan mogelijk leiden tot aanpassingen in deze normen en extra kosten voor bijvoorbeeld dijkversterkingen.

- ☐ **(On)mogelijkheden voor adaptatie:** bij de selectie van nieuwe locaties voor datacenters is het risico op overstroming een van de criteria. Echter, andere criteria, zoals toegang tot energievoorziening en waterbronnen, aanwezigheid van datakabels lijken belangrijker te zijn waardoor het klimaatrisico niet kan worden voorkomen.

5.6.4 Eindimpact

Eindimpact mens en cultuur

Voor het bepalen van de eindimpact zijn de volgende opties beschreven:

- ☐ **Laag:** < 10.000 getroffen mensen, 0 – 10 ernstig gewonden/doden, lokaal* en/of omkeerbare cultuurschade
- ☐ **Middel:** 10.000 – 100.000 getroffen mensen, 10 – 100 ernstig gewonden/doden, regionaal* en/of moeilijk omkeerbare cultuurschade
- ☐ **Hoog:** > 100.000 getroffen mensen, > 100 ernstig gewonden/doden, nationaal* en/of onomkeerbare cultuurschade

De eindimpact voor mens en cultuur van de verschillende klimaatrisico's is bepaald op laag. Uitval van ICT heeft geen directe impact op mensen, het zorgt niet voor doden of gewonden. Wel zijn er keteneffecten ten gevolge van uitval van ICT-voorzieningen, met name als deze impact hebben op kritieke communicatiediensten voor hulpverleners (zoals 112, C2000, mobiel netwerk). Echter, ook bij grootschalige (regionale of landelijke) verstoring gedurende meerdere uren zal het aantal ernstig gewonden/doden naar verwachting minder dan 10 blijven, op basis van eerdere verstoringen met bijv. 112.

Eindimpact: natuur en milieu

Voor het bepalen van de eindimpact natuur en milieu zijn de volgende opties beschreven:

- ☐ **Laag:** lokaal en/of omkeerbare schade op natuur en milieu
- ☐ **Middel:** regionaal en/of moeilijk omkeerbare schade op natuur en milieu
- ☐ **Hoog:** nationaal en/of onomkeerbare schade op natuur en milieu

De eindimpact voor natuur en milieu van de verschillende klimaatrisico's is bepaald op laag. Er zijn restricties voor datacenters t.a.v. het lozen van koelwater bij hogere temperaturen. Dit kan mogelijk betekenen dat datacenters moeten afschakelen als deze geen koelwater mag lozen. Als er tijdelijke uitzonderingen komen bij extreme omstandigheden, dan kan dit mogelijk lokaal impact hebben op natuur en milieu. Er is niet onderzocht wat mogelijke alternatieven zijn in deze situatie.

Eindimpact: economie

or het bepalen van de eindimpact economie zijn de volgende opties beschreven:

- ☐ **Laag:** < € 100 miljoen
- ☐ **Middel:** € 100 miljoen – 1 miljard
- ☐ **Hoog:** > € 1 miljard

De eindimpact op economie voor de verschillende klimaatrisico's is bepaald op 'laag'. Mogelijke uitzonderingen met grotere impact zijn:

- ☐ Grote regionale of landelijke stroomstoring die meerdere uren duurt. De eindimpact is dan 'middel' tot 'hoog' door de keteneffecten die optreden en de grote afhankelijkheid van de maatschappij van ICT en internet.

- Regionale overstrooming waarbij schade ontstaat aan gebouwen en apparatuur in een groter gebied. Herstel zal meerdere dagen tot weken duren, waardoor ICT-voorzieningen (masten, straatkasten, datacenters) een langere periode niet operationeel zijn.
- Keteneffecten bij uitval van individuele datacenters of kritieke ICT-voorzieningen binnen vitale sectoren (anders dan ICT). Deze zijn moeilijk in te schatten door de complexiteit binnen ketens en continue veranderingen binnen ketens van ICT-diensten en –voorzieningen. Keteneffecten kunnen uiteindelijk wel voor grote maatschappelijke ontwrichting zorgen als dit bijv. leidt tot uitval van vitale processen.

5.7 Beleidsboodschappen: opgaven voor de toekomst

In deze paragraaf zijn de restopgaven beschreven onder huidig beleid en de opgave voor toekomstige beleid om de klimaatrisico's (primair of secundair) verder te verminderen of cascade-effecten te verkleinen.

1. Economisch beleid

Vanuit economisch beleid is het wenselijk dat Nederland de positie van belangrijk digitaal knooppunt binnen Europa behoudt door voldoende ruimte te bieden voor (uitbreidingen) van hyperscale datacenters en (zee)datakabels naar andere delen van Europa. Vanuit andere, niet-economische overwegingen kan worden gekozen om te sturen op beperkingen ten aanzien van nieuwe hyperscale datacenters (van Amerikaanse BigTech bedrijven) in Nederland, gelet op de beperkte beschikbaarheid van duurzame elektriciteit en de congestie in (delen van) het elektriciteitsnetwerk. Daarnaast speelt de groeiende afhankelijkheid van Amerikaanse hyperscalers (met risico op politieke druk) een rol in het beleid t.a.v. BigTech en hyperscale datacenters. De beleidsopgave is om hier een goede afweging te maken tussen enerzijds het belang van een goede digitale infrastructuur, gekoppeld aan economische groei, en anderzijds de uitdagingen voor o.a. klimaatrisico's van (hyperscale) datacenters. De sector ICT is een private sector, dus de (klimaat)risico's van verstoringen liggen direct bij deze bedrijven. Indirect ondervinden burgers, overheid en bedrijven - als gebruikers van de digitale infrastructuur – negatieve gevolgen bij verstoringen van de digitale infrastructuur (keteneffecten).

2. Ruimtelijk beleid - Ruimtelijke spreiding en klimaatblootstelling verlagen

De markt voor datacenters zal de komende jaren sterk groeien, met name bij colocatie en hyperscalers, zowel binnen Nederland als binnen Europa. In Nederland is meer dan 70% van de colocatie datacenters in de Metropool Regio Amsterdam geconcentreerd. Onder huidig beleid blijft die concentratie bestaan. De opgave is:

- Klimaatblootstelling (overstrooming of wateroverlast en hitte/droogte) ruimtelijk te sturen en hierbij nieuwe of uitbreidende locaties bij voorkeur in laag-risicogebieden aan te wijzen. Denk hierbij aan:
 - Nieuwe locaties met laag risico op lokaal wateroverlast en in gebieden met lage kans op overstrooming,
 - Voor hitte en droogte in noordwesten van Nederland waar temperatuur gemiddeld lager is,
 - Zowel voor nieuwe locaties voor hyperscalers als voor een mogelijk tweede cluster buiten de MRA regio.

3. Duurzaamheid, duurzame digitalisering - Watergebruik en droogtebestendigheid borgen

Er is druk op zoet drinkwater. De sector verschuift voor (water)koeling al naar alternatieven als efficiëntere koeling en industrie/regen/effluent als bron. Als er niet wordt gestuurd is er risico op schaarste-gedreven beperkingen. De opgave is:

- ☐ Drinkwatergebruik voor koeling verder terugdringen en mogelijk op termijn wettelijk verbieden. Waterbedrijven kunnen alternatieve oplossingen bieden, bijv. door het leveren van industrieel water voor koeling.
- ☐ Water-positieve concepten stimuleren, d.w.z. maatregelen waardoor een locatie minder water onttrekt dan de locatie het systeem belast. Denk aan concepten met opvang van regenwater, dat na koeling kan worden gebruikt voor andere bedrijven zoals tuinbouwbedrijven.

Daarnaast zijn er opgaven vanuit de sector vanuit duurzaamheid, deze zijn niet direct gekoppeld aan klimaatrisico's, maar spelen wel een rol bij de ruimtelijke inrichting.

- ☐ Noodstroom moderniseren: waterstof i.p.v. diesel voor noodaggregaten. Mogelijk zouden datacenters op termijn volledig over kunnen gaan op stroomvoorziening via waterstofcellen. Transport van waterstof (bijv. via aansluitingen via waterstof/gasleidingen) naar (clusters) van datacenters en andere energie-intensieve industrie kan dan een randvoorwaarde zijn.
- ☐ Restwarmte van datacenters structureel benutten als randvoorwaarde bij vestiging of uitbreiding van (clusters van) datacenter(s).

4. Vitale infrastructuur - Energievoorziening en netcapaciteit binnen digitale infrastructuur robuust maken.

De IT-load en de vraag naar duurzame elektriciteit groeit voor colocatie datacenters en hyperscalers. Onder het huidige beleid is netcapaciteit de beperkende factor en vergroot uitvalrisico's bij schaarste. De opgave is:

- ☐ Directe, redundante aansluitingen voor grote locaties met minimale aanpassingen in het elektriciteitsnetwerk (dicht op hoofdnet, eigen onderstations) zodat de groei in netcapaciteit niet ten koste gaat van andere sectoren,
- ☐ Directe koppeling met duurzame opwekking (zon, wind, kernenergie waar politiek gekozen) om afstand tussen opwekking en gebruik door datacenters te beperken,
- ☐ Noodstroom moderniseren (waterstof i.p.v. diesel voor noodaggregaten) en brandstoflogistiek voor langdurige storingen, en indien mogelijk voorrang bij herstel in crisissituaties.

5. Vitale infrastructuur - Fysieke waterveiligheid en hittestress normeren

Onder huidige beleid zijn generieke kaders aanwezig, maar sectorspecifieke klimaateisen ontbreken vaak. Hierdoor kan de kwetsbaarheid uiteen blijven lopen. De opgave is:

- ☐ Landelijke (ontwerp)eisen voor datacenters t.a.v. waterveiligheid vastleggen. Denk hierbij aan minimale vloerhoogte t.o.v. lokale waterlijn/NAP, waterdichte doorvoeren, lekdetectie en afwatering.
- ☐ Voor bestaande clusters maatwerk te organiseren (bijvoorbeeld verplichte ophoging, waterdichte ontwerpstandaarden, nooddrainage en hittebestendige koeling).
- ☐ Europese/landelijke (ontwerp)eisen voor datacenters t.a.v. datacenterkoeling vastleggen. Denk hierbij aan setpoints voor koeling bij hittegolven, tropennachten en tijdslijnen t.a.v. migratie naar toekomstige koelsystemen zonder drinkwater.

6. Vitale infrastructuur - Weerbaarheid van vitale digitale ketens vergroten (Wwke)

De implementatie van Wwke en Cbw moet vitale processen beter beschermen, maar richt zich nu vooral op grote aanbieders. De opgave is:

- ☐ Naast natuurrampen ook andere klimaatrisico's expliciet meenemen in de risicobeoordeling bij Wwke: niet enkel natuurrampen, maar ook (lokale) overstroming door extreme lokale regenval, overstroming rivieren, langdurige droogte in combinatie met hitte, regionale stroomuitval.
- ☐ Ketenafhankelijkheden beperken (energievoorziening, telecom en cloud) door redundantie in te bouwen om single points of failure te voorkomen (dus bijvoorbeeld bij colocatie datacenters een tweede, fysiek andere locatie als uitwijk 'datacenter twinning').
- ☐ Regionale afspraken over prioritering in herstel na uitval (energie/telecom) voor digitale clusters.
- ☐ Via de Wwke én de Cbw kan hierop ook gestuurd worden vanuit wetgeving voor kritieke entiteiten in andere vitale sectoren, zodat zij gebruik maken van minimaal twee datacenters met geografische spreiding (primair/uitwijk niet in hetzelfde overstromingsbekken).

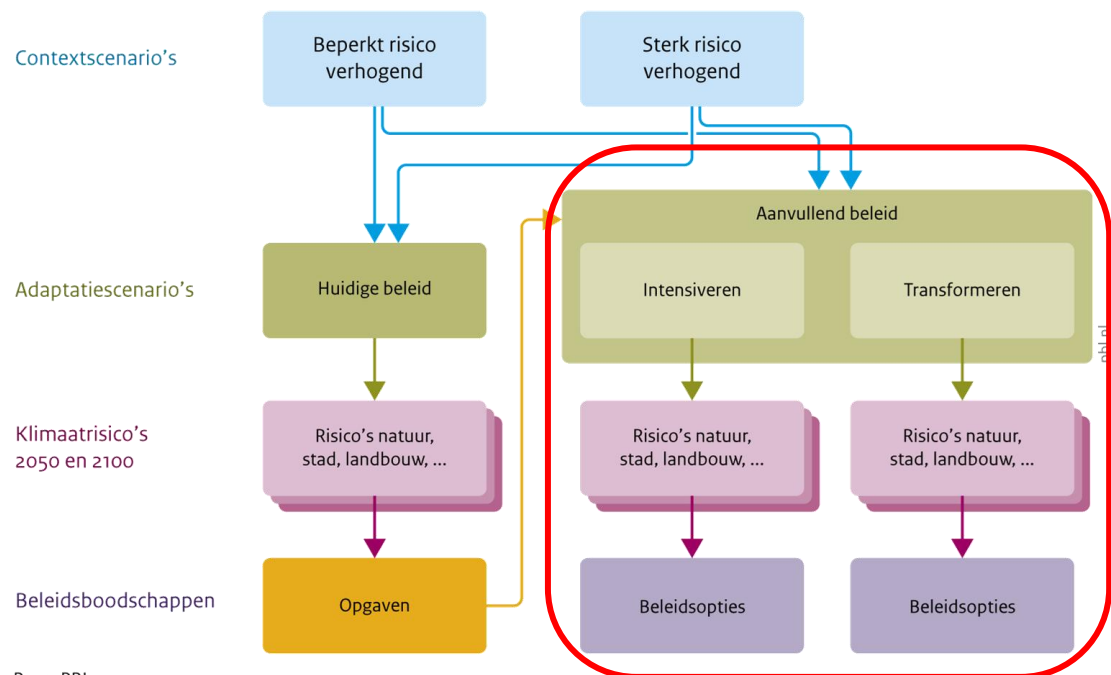
6 Klimaatrisicoanalyse digitale infrastructuur bij aanvullend beleid

In dit hoofdstuk is een analyse uitgevoerd van de mate waarin aanvullend beleid, via de twee adaptatiescenario's 'Intensiveren' en 'Transformeren' de klimaatrisico's in 2050 en 2100 kan reduceren, en wat dan de resterende risico's zijn. Op basis van deze analyse zijn de beleidsopties voor ICT beschreven.

Dit doen we aan de hand van vijf vragen:

1. Wat is de opgave d.w.z. het verschil tussen huidig en toekomstig beleid?
2. (In hoeverre) nemen de maatregelen van dit scenario de risico's weg en waarom?
3. Welke risico's blijven over en waarom?
4. Welke 'nieuwe' risico's treden op?
5. Wie zijn de winnaar en verliezers qua risico's bij dit adaptatiescenario? Zijn er kansen voor meekoppeling?

Verkenning toekomstige klimaatrisico's



Bron: PBL

Figuur 20 Scope van klimaatrisicoanalyse digitale infrastructuur bij aanvullend beleid (rode vak)

6.1 Adaptatiescenario's bij aanvullend beleid

In deze paragraaf zijn verschillende maatregelen beschreven voor aanvullend beleid vanuit de adaptatiescenario's 'transformeren' en 'intensiveren'. In lijn met de PBL-systematiek is 'transformeren' gericht op het verlagen van de blootstelling (waar en hoe we datacenters toestaan) en 'intensiveren' op het verlagen van de kwetsbaarheid en gevoeligheid (technische en organisatorische maatregelen op bestaande en nieuwe locaties).

6.1.1 Transformeren

Binnen dit scenario zijn de volgende maatregelen mogelijk t.a.v. ruimtelijke spreiding:

1. Geen nieuwe locaties aanwijzen voor hyperscale datacenters in Nederland (MT-S1).
2. Maatregelen ter verbetering van geografische spreiding door bijvoorbeeld een tweede datacentercluster in Nederland naast MRA (nu >70%). Hiermee worden verstoringen door regionale klimaatrisico's in MRA (regionale stroomuitval, regionale overstroming, regionaal watertekort) voor Nederland als geheel kleiner. Ruimtelijke spreiding kan uiteraard ook betekenen om een tweede cluster buiten Nederland te gebruiken, bijv. in Duitsland, België of Frankrijk.

De eerste maatregel betekent vanuit economisch en ruimtelijk beleid een aanscherping van het huidige beleid t.a.v. de vestiging van nieuwe hyperscalers in Nederland. Omdat de vraag naar duurzaam opgewekte elektriciteit door AI en cloud sterk toeneemt, kan het rationeel zijn een deel van de toekomstige hyperscale-groei te laten landen in Europese regio's waar meer ruimte, meer duurzame energie en lagere klimaatrisico's zijn (bijv. Scandinavië). In Nederland krijgen andere sectoren dan toegang tot duurzaam opgewekte elektriciteit zoals met zon en wind. Hiermee kan de alsmaar groeiende vraag naar duurzame energie van datacenters worden verplaatst naar deze landen en is er in Nederland ruimte voor gebruik van duurzame energie voor groei van andere economische activiteiten. Bij een verbod op nieuwe hyperscalers in Nederland verminderen uiteraard ook de bijbehorende klimaatrisico's voor Nederland, bijv. door verstoringen bij lokale overstromingen of door koelproblemen bij beperkingen in (drink)watergebruik bij droogte en/of beperkingen t.a.v. lozing van koelwater bij te warm oppervlaktewater. Het probleem wordt hiermee deels verplaatst naar andere landen binnen de EU.

Aan de andere kant investeren juist hyperscalers – vanuit hun schaalgrootte en door huidig beleid - ook zelf in duurzame energie en alternatieve waterbronnen via regenwater en oppervlaktewater, doordat waterbedrijven al geen drinkwater meer leveren voor koeling. Hierdoor presteren hyperscalers vanuit duurzaamheid vaak beter dan de vele, kleine datacenters. Het volledig weren van nieuwe hyperscalers in Nederland kan dus ook betekenen dat het gemiddelde duurzaamheidsniveau van de Nederlandse datacenterpopulatie daalt.

Een ander tegenargument is dat Europa minder afhankelijk wil zijn van de Amerikaanse cloud-providers en dus zal Europa ruimte moeten geven aan nieuwe Europese partijen. Het is niet duidelijk hoe de Europese Unie en Nederland dit wil vormgeven, bijv. voor aanwijzing en selectie van nieuwe locaties voor duurzame Europese hyperscale datacenters.

6.1.2 Intensiveren

Het uitgangspunt bij dit scenario is dat groei van digitale infrastructuur mogelijk blijft, gelet op het belang van digitale infrastructuur binnen Nederland en Europa. Uitbreiding op huidige en nieuwe locaties voor hyperscalers en datacenters blijft mogelijk, maar dan alleen gekoppeld aan technische maatregelen vanuit ruimtelijk beleid, duurzaamheid en vitale infrastructuur.

Hierna volgen de belangrijkste klimaatrisico's voor datacenters, met mogelijke maatregelen.

1. Overstromingen, lokale wateroverlast
 - a. Bij selectie van nieuwe locaties voor hyperscalers of bij clusters van datacenters rekening houden met het risico op overstromingen. Nieuwe locaties selecteren met expliciete weging van klimaatrisico's (MI-O1).
 - b. Aanvullende wetgeving met maatregelen tegen lokale wateroverlast bij bouw nieuwe datacenters (denk aan opvang van overtollig regenwater, maatregelen tegen lokale waterhoogte van 10-50 cm, etc.) (MI-O2).
 - c. Aanvullende wetgeving met maatregelen tegen lokale wateroverlast bij bestaande datacenters (MI-O3)
2. Watertekort bij langdurige droogte of hitte
 - a. Restricties laagwaardig drinkwatergebruik voor koeling verder aanscherpen, ook voor kleinere datacenters. Deze maatregel zal niet alleen voor de sector ICT gelden, maar ook voor andere sectoren met laagwaardig drinkwatergebruik (MI-W1).
 - b. Stimuleren van het gebruik van alternatieven voor koeling met drinkwater (laagwaardig gebruik van drinkwater) voor datacenters, bijv. door verhoging van tarieven voor laagwaardig gebruik van drinkwater of door subsidies vanuit duurzaamheid in zogeheten 'water-positieve' oplossingen. Hyperscalers maken al gebruik van deze oplossingen door opvang van regenwater of het gebruik van gezuiverd oppervlaktewater. Opvang van regenwater of het gebruik van gezuiverd oppervlaktewater voor koeling vereist - vanuit schaal-grootte en investering - lokale samenwerking tussen aanbieders van deze oplossingen, de afnemers van koelwater (clusters van datacenters en andere industrie) en mogelijk andere sectoren die het afgevoerde water na koeling gebruiken voor bijv. land- en tuinbouw. Ook zijn alternatieve oplossingen mogelijk voor datacenters, zoals gesloten koelsystemen of het gebruik van gezuiverd industrieel water (MI-W2).
 - c. Aanscherpen eisen van WUE voor datacenters (hyperscalers, colocatie en single-tenant). Hiermee wordt efficiënter gebruik van drinkwater voor koeling verplicht. Mogelijk zijn regio-afhankelijke WUE eisen nodig, met bijv. strengere eisen voor locaties in een gematigd klimaat zoals Noordwest Europa (MI-W3).
3. Stroomuitval
 - a. Vanuit het risico op uitval van de elektriciteitsvoorziening kunnen maatregelen worden genomen om dit risico voor hyperscalers en grotere (clusters van) datacenters te beperken, bijvoorbeeld door 'directe' aansluiting op het hoofdstroomnetwerk vanuit windmolenparken op zee, zonneparken en/of kerncentrales, of gebruik van lokaal opgeslagen waterstof voor elektriciteits-opwekking in brandstofcellen voor noodstroomvoorzieningen (MI-S1). Voor

kleinere single-tenant datacenters is uitwijk naar een tweede (colocatie of cloud) datacenter noodzakelijk, naast investeringen in noodstroomvoorzieningen.

- b. Beleidsmaatregelen om gevolgen van stroomonderbrekingen van vitale aanbieders binnen de digitale infrastructuur te beperken: denk aan voorrang bij herstel stroomvoorziening, 'directe' aansluitingen voor vitale aanbieders/ hyperscale datacenters op hoofdstroomnetwerk, verplichte back-up via noodstroom (met waterstofcellen) tot 72 uur voor vitale aanbieders (MI-S2).
4. Algemeen/vitale infrastructuur
- a. Verminderen kwetsbaarheid van keteneffecten bij verstoring digitale infrastructuur door alle klimaatrisico's expliciet op te nemen in de risicoanalyse voor van de Wwke (MI-A1). Bij de Wwke en Cbw is het belangrijk dat ook klimaatrisico's (breder dan natuurrampen) worden opgenomen in de nieuwe wetgeving. Hierdoor kunnen op basis van de Wwke en de Cbw aanvullende maatregelen worden verplicht voor specifieke klimaatrisico's
 - b. Andere opties zijn het beter informeren van kleinere organisaties met vitale functies (en onderliggende digitale infrastructuur) om maatregelen te nemen om gevolgen van verstoringen door klimaatrisico's te beperken (best-practices) (MI-A2).

6.2 Klimaatrisicoanalyse bij aanvullend beleid

6.2.1 Transformeren

1. Wat is de opgave d.w.z. het verschil tussen huidig en toekomstig beleid?

De opgaven voor het huidige beleid zijn beschreven in paragraaf 5.7. Hierbij is gekeken vanuit verschillende beleidsthema's (economisch, ruimtelijk, duurzaamheid en vitale infrastructuur) omdat beleidsmaatregelen een afweging zijn vanuit meerdere thema's. In deze paragraaf is gekeken naar beleidsmaatregelen om verstoringen in de digitale infrastructuur ten gevolge van klimaatrisico's te beperken, met een afweging tussen de beleidsthema's.

In het huidige beleid bepaalt de Rijksoverheid of en waar nieuwe hyperscalers gevestigd mogen worden. Lokale overheden hebben zeggenschap over kleinere datacenters. In het huidige beleid is niet vastgelegd dat er in Nederland geen nieuwe locaties kunnen worden aangewezen voor hyperscalers. Men ziet wel dat hyperscalers uitbreiden door satellietlocaties (kleinere datacenters) te bouwen of gebruiken (colocatie) dicht bij de locatie van een hyperscale datacenter. Bij het beleid spelen meerdere afwegingen een rol, zoals hierboven beschreven. Vanuit de klimaatrisico's voor datacenters zorgt het beperken van (uitbreidingen van) hyperscalers ervoor dat de risico's binnen Nederland minder worden, doordat er minder hyperscale datacenters zijn. Hierbij dient opgemerkt te worden dat (vanuit economisch perspectief) een nadere analyse nodig is om te bepalen of het toenemende elektriciteitsverbruik van hyperscalers zorgt voor beperkte groei in andere sectoren, of dat de problemen van netcongestie los moet worden gezien hiervan.

2. (In hoeverre) nemen de maatregelen van dit scenario de risico's weg en waarom?

Het klimaatrisico wordt verplaatst naar een ander land binnen Europa of zelfs buiten Europa. Het klimaatrisico kan lager worden als het om nieuwe locaties gaat met lagere klimaatrisico's zoals in Noorwegen, Zweden, Finland. Echter, Nederland is een aantrekkelijk land voor hyperscalers gezien de geografische ligging (gematigd klimaat, toegang tot datakabels en duurzame energie (wind, zonne-energie en/of kernenergie) en het politieke en economische klimaat.

3. Welke risico's blijven over en waarom?

Voor Nederland blijven er geen klimaatrisico's over, wel binnen Europa. Bij vestiging van nieuwe hyperscale datacenters in bijv. Scandinavië zal het klimaatrisico naar verwachting afnemen (koeler klimaat, minder kans op droogte).

4. Welke 'nieuwe' risico's treden op?

Er zijn geen nieuwe klimaatrisico's, deze worden door Nederland verplaatst naar andere (Noordelijke) landen binnen Europa. Wel zal er sprake zijn van een verslechtering van de positie van Nederland binnen Europa, en in het bijzonder de Metropool Regio Amsterdam, als digitaal knooppunt. Voor Europa bestaat er een risico t.a.v. digitale soevereiniteit indien hyperscalers uiteindelijk moeten kiezen voor locaties buiten Europa door de beperkingen door wetgeving ten aanzien van duurzaamheid en vitale aanbieders (Wwke, Cbw), naast de bestaande wetgeving vanuit de Digital Market Act (DMA) en de Digital Services Act (DSA). Ook wordt Nederland voor zijn digitale infrastructuur meer afhankelijk van andere landen.

Verder vallen investeringen weg van cloudbaanbieders in nieuwe infrastructuur voor duurzame energie en zijn water-positieve oplossingen en oplossingen voor hergebruik van restwarmte niet meer beschikbaar.

5. Wie zijn de winnaar en verliezers qua risico's bij dit adaptatiescenario? Zijn er kansen voor meekoppeling?

Bij dit scenario wordt het probleem van klimaatrisico's verplaatst naar andere EU-landen, die samen nog steeds sterk afhankelijk blijven van de digitale infrastructuur van cloudbaanbieders. Het risico neemt voor Europa als geheel wel af indien hyperscalers zich vestigen op locaties binnen Europa met kleinere klimaatrisico's. Echter, de keuze voor nieuwe locaties door cloudbaanbieders wordt nu voor een (zeer) klein deel bepaald vanuit klimaatrisico's. Toegang tot duurzame energiebronnen, nu en in de toekomst, en een stabiele overheid, zijn op dit moment belangrijkere criteria. Er zijn geen kansen op meekoppeling geïdentificeerd.

6.2.2 Intensiveren

1. Wat is de opgave d.w.z. het verschil tussen huidig en toekomstig beleid?

De opgaven voor het huidige beleid zijn beschreven in paragraaf 5.7. Hierbij is gekeken naar de opgave vanuit verschillende beleidsthema's (economisch, ruimtelijk, duurzaamheid en vitale infrastructuur) aangezien beleidsmaatregelen een afweging vereisen vanuit meerdere thema's. De opgave is om een afweging te maken in beleidsmaatregelen vanuit de verschillende beleidsthema's, met aandacht voor de klimaatrisico's op de lange termijn.

2. In hoeverre nemen de maatregelen van dit scenario de risico's weg en waarom?

Hieronder volgen de verschillende mogelijke maatregelen bij de belangrijkste klimaatrisico's voor datacenters, zoals beschreven in paragraaf 5.2.2, vervolgd met in hoeverre deze maatregelen de risico's wegnemen, en waarom.

1. Overstromingen, lokale wateroverlast
 - a. Bij selectie van nieuwe locaties voor hyperscalers of bij clusters van datacenters rekening houden met het risico op overstromingen. Nieuwe locaties selecteren met expliciete weging van klimaatrisico's.
 - i. Het klimaatrisico wordt beperkt lager, maar geldt enkel voor nieuwe locaties. Het effect is dus beperkt, aangezien het niet risico's van bestaande datacenters wegneemt. Opmerking: vanuit huidig beleid worden wel bredere maatregelen genomen om het risico op overstroming te beperken door dijkverzwaring etc. waardoor het risico in 2100 in grote delen van Nederland lager is dan nu en in 2050.
 - b. Aanvullende wetgeving met maatregelen tegen lokale wateroverlast bij bouw nieuwe datacenters of bij bestaande datacenters (denk aan opvang van overtollig regenwater, maatregelen tegen lokale waterhoogte van 10-50 cm, etc.).
 - i. Het klimaatrisico wordt beperkt lager, in het geval maatregelen enkel gelden voor bouw van nieuwe datacenters.
 - ii. Het klimaatrisico wordt sterk lager als de maatregelen voor alle bestaande datacenters gaan gelden, bijv. door vastgestelde maatregelen voor (klimaat)risico's vanuit de Wwke.
2. Watertekort bij langdurige droogte of hitte
 - a. Restricties (verbod op) laagwaardig drinkwatergebruik voor koeling verder aanscherpen, ook voor kleinere datacenters. Deze maatregel zal niet alleen voor de sector ICT gelden, maar ook voor andere sectoren met laagwaardig drinkwatergebruik.
 - i. Hiermee wordt het indirecte klimaatrisico door restricties op laagwaardig drinkwatergebruik bij langdurige droogte volledig weggenomen. Na invoering van deze maatregel zullen bedrijven een bepaalde periode (meerdere jaren) nodig hebben om over te stappen naar alternatieven voor laagwaardig drinkwatergebruik (regenwater, industrieel water, zuivering oppervlaktewater). Deze maatregel geldt alleen voor datacenters die drinkwater gebruiken voor koeling, d.w.z. colocatie datacenters (ca. 80%) en single-tenant datacenters (onbekend, naar verwachting >80%)
 - b. Stimuleren van het gebruik van alternatieven voor koeling met drinkwater (laagwaardig gebruik van drinkwater) voor datacenters, bijv. door verhoging van tarieven voor laagwaardig gebruik van drinkwater of door subsidies vanuit duurzaamheid in zogeheten 'water-positieve' oplossingen. Hyperscalers maken al gebruik van deze oplossingen via opvang van regenwater of gebruik van gezuiverd oppervlaktewater. Opvang van regenwater of gebruik van gezuiverd oppervlaktewater voor koeling vereist - vanuit schaalgrootte en investering - lokale samenwerking tussen aanbieders van deze oplossingen, de afnemers van koelwater (clusters van datacenters en andere industrie) en mogelijk andere sectoren die het afgevoerde water na koeling gebruiken voor bijv. land- en tuinbouw. Ook zijn alternatieve oplossingen mogelijk voor datacenters, zoals gesloten koelsystemen of gebruik van gezuiverd industrieel water.

- i. Het risico wordt beperkt tot sterk lager, afhankelijk van de financiële haalbaarheid.
 - c. Aanscherpen eisen ten aanzien van efficiënt watergebruik (bijv. via WUE) voor datacenters (hyperscalers, colocatie en single-tenant). Hiermee wordt efficiënter gebruik van drinkwater voor koeling verplicht. Mogelijk zijn regio-afhankelijke WUE eisen nodig, met bijv. strengere eisen voor locaties in een gematigd klimaat zoals Noordwest Europa.
 - i. Het risico wordt beperkt lager, watergebruik kan beperkt worden verminderd. Bovendien zijn de eisen voor datacenters in een gematigd klimaat eenvoudiger te halen, doordat er minder koeling (en dus drinkwater) nodig is.
- 3. Stroomuitval
 - a. Vanuit het risico op uitval van elektriciteitsvoorziening kunnen maatregelen in het elektriciteitsnetwerk worden genomen om dit risico voor hyperscalers en datacenters te beperken door 'directe' aansluiting op het hoofdstroomnetwerk bijv. vanuit windmolenparken op zee, zonneparken en/of kernenergie, of toegang tot waterstof voor lokale elektriciteitsopwekking (brandstofcellen).
 - i. Het risico wordt beperkt tot sterk lager, afhankelijk van de technische en financiële haalbaarheid van de maatregelen. De maatregel is enkel haalbaar voor een beperkt aantal datacenters: hyperscalers en clusters van colocatie datacenters. Voor single-tenant is deze maatregel niet haalbaar.
 - b. Beleidsmaatregelen om gevolgen van stroomonderbrekingen van vitale aanbieders binnen de digitale infrastructuur te beperken: denk aan voorrang bij herstel stroomvoorziening, 'directe' aansluitingen voor vitale aanbieders/ hyperscale datacenters op redundant hoofdstroomnetwerk, verplichte back-up via noodstroom (met waterstofcellen, tot 72 uur) voor vitale aanbieders.
 - i. Het risico wordt beperkt lager, afhankelijk van de technische en financiële haalbaarheid van de maatregelen. Een deel van de maatregelen is enkel haalbaar voor een klein aantal datacenters (hyperscalers) of voor clusters van colocatie datacenters. Voor single-tenant is noodstroom haalbaar, voorrang bij herstel is technisch niet realistisch door het grote aantal single-tenant datacenters en doordat herstel in het distributienet enkel geografisch mogelijk is, en niet per aansluiting.
- 4. Algemeen/vitale infrastructuur
 - a. Verminderen kwetsbaarheid van keteneffecten bij verstoring digitale infrastructuur door alle klimaatrisico's expliciet op te nemen in de risicoanalyse vanuit de Wwke. Bij de Wwke en Cbw is het belangrijk dat ook klimaatrisico's - breder dan natuurrampen – worden opgenomen in de nieuwe wetgeving. Hierdoor kunnen o.b.v. de Wwke en de Cbw aanvullende maatregelen worden verplicht voor deze risico's.
 - i. Klimaatrisico's worden beperkt tot sterk lager, afhankelijk van de weging van klimaatrisico's t.o.v. andere risico's. Ook is het afhankelijk van de partijen die worden aangewezen als vitale aanbieders.
 - b. Andere opties zijn het beter informeren van kleinere organisaties met vitale functies (en onderliggende digitale infrastructuur) om maatregelen te nemen om gevolgen van verstoringen door klimaatrisico's te beperken (best-

practices). Dit kan vanuit een breder perspectief, d.w.z. vanuit alle risico's voor uitval digitale infrastructuur (klimaat, cyber, technisch, geografisch)

- i. Klimaatrisico's worden beperkt lager. Het merendeel van de vitale aanbieders neemt al maatregelen voor klimaatrisico's vanuit een bredere risicoanalyse t.a.v. continuïteit. Deze maatregel heeft enkel effect op de kleinere organisaties. Mogelijk dat deze partijen versneld overstappen naar colocatie datacenters of hyperscalers.

3. Welke risico's blijven over en waarom?

Overstroming: de risico's worden met de aanvullende maatregelen niet geheel weggenomen, maar de restrisico's blijven laag.

Watertekort (als secundair effect bij langdurige droogte/hitte): bij gebruik van oppervlaktewater als alternatieve waterbron zijn er nog restrisico's, namelijk restricties op gebruik oppervlaktewater (bij lage afvoer) en risico op het niet mogen lozen van koelwater op oppervlaktewater bij te hoge temperaturen. Hier zijn dan weer aanvullende maatregelen nodig.

Stroomuitval: de risico's worden met de aanvullende maatregelen niet geheel weggenomen, maar de restrisico's blijven laag.

Algemeen/vitale infrastructuur: de Wwke en de Cbw gelden enkel voor kritieke entiteiten. Er blijven hierdoor wel klimaatrisico's over voor niet-kritieke entiteiten met een eigen digitale infrastructuur, maar de impact zal lager zijn aangezien deze niet als vitaal zijn aangemerkt.

4. Welke 'nieuwe' risico's treden op?

Er zijn geen nieuwe klimaatrisico's geïdentificeerd.

5. Wie zijn de winnaar en verliezers qua risico's bij dit adaptatiescenario? Zijn er kansen voor meekoppeling?

De maatregelen zorgen voor het beperken van klimaatrisico's en dus een hogere beschikbaarheid van de digitale infrastructuur, met name voor vitale aanbieders en hyperscalers. De winnaars zijn daarom met name de grote en vitale aanbieders met schaal om te kunnen voldoen aan Wwke en Cbw. Deze partijen opereren in een Europese of globale markt en hebben hun infrastructuur al breed verspreid over Europa en/of andere regio's. Deze partijen kunnen vanuit schaalgrootte eenvoudiger maatregelen nemen of hebben die al genomen waardoor zijn het beste presteren vanuit duurzaamheid en beschikbaarheid. Met de aanvullende maatregelen zullen met name kleinere single-tenant en colocatie datacenters de verliezers zijn, omdat zij relatief hogere kosten zullen moeten maken, of doordat organisaties en bedrijven versneld moeten overstappen naar grotere colocatie of hyperscale datacenters om aan de wetgeving te kunnen voldoen. Nederland als geheel is hierdoor beter af, gezien een hogere weerbaarheid van de digitale infrastructuur, ook tegen klimaatrisico's.

6.3 Beleidsboodschappen met beleidsopties voor aanvullend beleid

6.3.1 Transformeren

In

Tabel 5 is het effect van de maatregel beschreven voor de maatregelen voor transformeren, zoals beschreven in paragraaf 6.1.1.

Tabel 4 Overzicht van effect van maatregelen voor transformeren voor contextscenario's beperkt en sterk risicoverhogend.

Maatregel	2050 Beperkt	2050 Sterk	Type datacenters
Transformeren – Ruimtelijke spreiding			
Verbod hyperscalers in NL (MT-S1)	Risico volledig weggenomen	Risico volledig weggenomen	Hyperscalers, enkel voor NL, niet voor EU
2 ^e datacenter cluster, naast MRA (MT-S2)	Risico beperkt verminderd	Risico sterk verminderd	Colocatie

De belangrijkste beleidsboodschappen zijn hieronder beschreven.

- Een hoogwaardige digitale infrastructuur in Nederland en Europa is en blijft belangrijk voor economische groei. Een volledig nationaal verbod op nieuwe hyperscale datacenters vermindert de klimaatrisico's voor Nederland, maar leidt tot verplaatsing van de opgave naar andere EU-landen en kan de Nederlandse positie binnen de Europese digitale infrastructuur verzwakken. Daarom ligt het meer voor de hand om geografische spreiding van (hyperscale) datacenters binnen Europa af te stemmen en daarnaast via nationaal ruimtelijk beleid binnen Nederland vorm te geven met specifieke aandacht voor toegang tot duurzame energie (kernenergie, waterstof) gezien de sterke groei in elektriciteitsvraag van datacenters en 'AI factories'.
- Daarnaast is een verbetering van de geografische spreiding van datacenters wenselijk om de systeemkwetsbaarheid voor regionale klimaatincidenten te verkleinen, met een tweede nationale cluster naast MRA (nu >70%). De risico's op verstoringen t.g.v. regionale klimaatrisico's in de MRA-regio, zoals regionale uitval van elektriciteitsvoorziening, regionale overstromingen of regionale watertekorten worden hiermee voor Nederland als geheel sterk verminderd. Geografische spreiding is uiteraard ook mogelijk binnen Europa naar andere datacenterclusters in buurlanden

6.3.2 Intensiveren

In onderstaande tabel is het effect van de aanvullende maatregelen onderling vergeleken. In

Tabel 5 is het effect van de maatregel beschreven voor de maatregelen voor intensiveren, zoals beschreven in paragraaf 6.2.2.

Tabel 5 Overzicht van effect van maatregelen voor intensiveren voor contextscenario's beperkt en sterk risicoverhogend.

Maatregel	2050 Beperkt	2050 Sterk	Type datacenters
Intensiveren – Overstroming			
Nieuwe datacenters in gebied laag risico (MI-O1)	Risico beperkt verminderd	Risico beperkt verminderd	Hyperscalers, colocatie
Maatregelen lokale wateroverlast datacenters bij nieuwbouw (MI-O2)	Risico beperkt verminderd	Risico beperkt verminderd	Hyperscalers, colocatie, single tenant
Maatregelen lokale wateroverlast Bij bestaande datacenters vanuit Wwke (MI-O3)	Beperkt tot sterk	Sterk	Hyperscalers, colocatie
Intensiveren – Watertekort			
Verbod laagwaardig drinkwatergebruik (MI-W1)	Risico volledig weggenomen	Risico volledig weggenomen	Colocatie, single tenant
Stimuleren alternatieven voor drinkwater- of watergebruik (MI-W2)	Risico beperkt verminderd	Risico beperkt tot sterk verminderd	Colocatie, single tenant
Efficiënter watergebruik voor koeling (MI-W3)	Risico beperkt verminderd	Risico beperkt verminderd	Colocatie, single tenant
Intensiveren - Stroomuitval			
Maatregelen elektriciteitsnetwerk (MI-S1)	Risico beperkt verminderd	Risico beperkt tot sterk verminderd	Hyperscalers, clusters colocatie
Gevolgen beperken (MI-S2)	Risico beperkt verminderd	Risico beperkt verminderd	Hyperscalers, colocatie
Intensiveren Algemeen (vitale infra)			
Verminderen kwetsbaarheid van keteneffecten via Wwke (MI-A1)	Risico beperkt verminderd	Risico beperkt tot sterk verminderd	Vitale aanbieders: hyperscalers, deel van colocatie en beperkt deel single tenant
Informereren klimaatrisico's (MI-A2)	Risico beperkt verminderd	Risico beperkt verminderd	Single tenant, deel van colocatie

De belangrijkste beleidsboodschappen zijn:

- Onderzoek de mogelijkheid op een volledig verbod op laagwaardig drinkwatergebruik voor datacenters en de overstap naar alternatieven (industriële water, regen- of oppervlaktewater). Mogelijk dat hiervoor ook financiële stimulering vanuit de overheid (subsidies en/of hogere tarifiering voor laagwaardig drinkwatergebruik) voor de overstap naar alternatieven wenselijk is, zowel voor de digitale sector als voor andere sectoren die getroffen worden.
- Neem klimaatrisico's expliciet mee in het ruimtelijk beleid en in de uitvoering van de Wet weerbaarheid kritieke entiteiten (Wwke). Hiermee is het mogelijk om sector brede maatregelen voor de digitale infrastructuur (met vitale telecom en cloudbaanbieders) te nemen om de verschillende klimaatrisico's tot 2050 te beperken, bijv. bij lokale wateroverlast, regionale droogte/hitte en regionale stroomuitval (t.g.v. klimaatrisico's). Door verdere aanscherping van (Europese) wettelijke restricties voor de gehele sector (door deze op de korte en middellange termijn strikter worden, lijken de klimaatrisico's tot 2050 (en mogelijk zelfs tot 2100) goed te mitigeren.
- Richt een maatstaf en monitoring in, zodat naleving en het effect van maatregelen voor de verschillende klimaatrisico's over de jaren heen gevolgd kan worden.
- Het effect van het beleid is groter naarmate klimaatrisico's groter zijn.

7 Sectorspecifieke infrastructuur

In deze paragraaf kijken we naar sectorspecifieke digitale infrastructuur die wordt gebruikt binnen de sectoren openbare orde en veiligheid, elektriciteitsvoorziening, gezondheidszorg en transport. Organisaties zijn zelf verantwoordelijk voor bijv. aanleg, onderhoud en beheer van deze digitale infrastructuur. Deze organisaties maken uiteraard ook gebruik van de generieke digitale infrastructuur, zoals beschreven in hoofdstuk 3, maar in deze paragraaf kijken we naar deze eigen infrastructuur en eventuele extra klimaatrisico's.

De resultaten uit dit hoofdstuk zijn gebaseerd op een combinatie van literatuur en interview. De interviews afgenomen aan de hand van een reeks gerichte vragen. De kern van deze vragen lag bij het beheer van ICT-onderdelen, verantwoordelijkheden, ervaringen met uitval en back-upmaatregelen, kwetsbaarheid van infrastructuur voor verschijnselen als direct gevolg van klimaatverandering, bestaande risico-inventarisaties, voorbereiding op langdurige stroomuitval, en het bestaande beleid binnen de organisaties, de sector en de overheid. Ook werd gevraagd naar rapportages over de rol van ICT, de behoefte aan aanvullend beleid en eventuele doorverwijzingen.

7.1 Openbare orde en veiligheid

7.1.1 Digitale infrastructuur OOV

Binnen de sector Openbare Orde en Veiligheid (OOV) zijn meerdere organisaties actief, zoals hulpdiensten (politie, brandweer en ambulance), Koninklijke marechaussee, verschillende lokale en provinciale organisaties in de 25 veiligheidsregio's, en organisaties in de landelijke crisisstructuur. Binnen de sector OOV wordt gebruik gemaakt van zowel de openbare digitale infrastructuur (bijvoorbeeld voor (mobiele) telefonie en internet) als van verschillende besloten netwerken, zoals C2000 voor hulpverleners en de NoodCommunicatieVoorziening (NCV) voor crisisorganisaties binnen de overheid en vitale aanbieders (zoals drinkwaterbedrijven, waterschappen, elektriciteitsleveranciers). Voor de bereikbaarheid van hulpdiensten, via 112, is de overheid afhankelijk van de vaste en mobiele telecomnetwerken in Nederland, en voor het informeren van burgers via NL-Alert van de mobiele netwerken.

7.1.2 Klimaatrisico's sectorspecifieke infrastructuur

De besloten netwerken binnen de OOV, zoals C2000 en NCV, verschillen qua technische elementen niet wezenlijk van de digitale infrastructuur, zoals hierboven beschreven. Het C2000-netwerk maakt bijv. ook gebruik van masten/opstelpunten voor actieve C2000-zenders, van glasvezelkabels en van (single-tenant of colocatie) datacenters voor de centrale netwerkkapapparatuur voor C2000. Daarnaast maakt men gebruik van lokale data- en ICT-netwerken op bijv. meldkamers en regionale crisiscentra. NCV wordt gebruikt binnen de landelijke crisisstructuur voor interne communicatie (telefonie, data) als de openbare

telecomnetwerken niet meer werken. Binnen zowel het NCV als C2000 vormen noodstroomvoorzieningen een belangrijke component voor continuïteit bij stroomuitval.

De klimaatrisico's zijn voor deze besloten netwerken daarom niet wezenlijk anders. Het belangrijkste onderscheid is dat de overheid zelf (OOV- en crisisorganisaties), en vitale partners verantwoordelijk zijn voor de weerbaarheid van deze besloten netwerken en zelf maatregelen moeten nemen om de risico's op uitval te beperken. Dit kan door voldoende redundantie in deze netwerken te gebruiken, door gebruik van terugval op alternatieven of door aanvullende maatregelen tegen (klimaat)risico's te nemen.

Binnen de sector OOV zijn verschillende activiteiten en werkgroepen die specifiek kijken naar klimaatrisico's. Het programma Klimaatveiligheid van het Nederlands Instituut Publieke Veiligheid (NIPV) is hier een voorbeeld van. Dit programma heeft tot doel om (beter) zicht te krijgen op de mogelijkheden en onmogelijkheden voor een veilige en weerbare samenleving bij klimaatverandering nu en in de toekomst. Het programma is een samenwerking tussen de veiligheidsregio's, NIPV, Ministerie van Justitie en Veiligheid en KNMI. In opdracht van NIPV heeft kennisinstituut Deltares in 2024 10 knelpunten en 10 aanbevelingen geïdentificeerd in de (bovenregionale) samenwerking van crisisresponsorganisaties [79]. De uitkomsten zijn opgehaald in vier workshops (hitte, droogte, wateroverlast, stormvloed) waaraan werd deelgenomen door een groot aantal veiligheidsregio's, ministeries, politie, Rode Kruis, Rijkswaterstaat, RIVM, KNMI, KPN, Koninklijke Landmacht en Alliander. In de workshops is met name gekeken in hoeverre crisisorganisaties voorbereid zijn op incidenten die optreden van een klimaatrisico, zoals felle en grotere natuurbranden of lokale overstromingen.

Uit alle vier workshops bleek verder de sterke afhankelijkheid van elektriciteit en telecom/ICT voor de bereikbaarheid en het optreden van responsorganisaties. De aanbeveling voor dit knelpunt is inzetten op kennis rondom mogelijke cascade-effecten en wat die betekenen voor de crisisrespons door middel van modelstudies en oefeningen met dergelijke incidentstapelingen met uitval van elektriciteit en communicatie, zoals het falen van pompen en gemalen tijdens een overstroming of wateroverlast.

7.1.2.1 Keten- of cascade-effecten bij klimaatrisico's

De sterke afhankelijkheid van telecom en/of elektriciteit zijn bekend, maar het in kaart brengen van de cascade-effecten bij optreden van klimaatrisico's voor responsorganisaties zijn complex, zeker indien meerdere ketens en sectoren betrokken zijn. Het NIPV heeft een studie laten uitvoeren met leerpunten uit crises bij klimaatverandering en extreem weer [80]. In de studie zelf zijn 14 crises beschreven. In geen van de cases werd uitval van (delen in de) digitale infrastructuur genoemd, en waren er dus geen cascade-effecten. Hiervoor wordt verwezen naar een studie uit 2011 van Eeten et al. [81] naar cascade-effecten. In de studie is men nagegaan in hoeverre verstoringen (in de periode medio 2008 tot 2011) als gevolg van de (veronderstelde) toegenomen complexiteit van de samenleving zich ook daadwerkelijk meer zogeheten 'cascade-effecten' hebben voorgedaan ten gevolge van een gekoppeld falen in kritische infrastructuren. Daarvoor is gebruik gemaakt van een databank van vele honderden verslagen van incidenten in verschillende kritische infrastructuren. De primaire analyse was gericht op 830 Nederlandse incidenten; 4239 buitenlandse rapporten dienden als vergelijking (secundaire analyse). Van de 830 Nederlandse casus zagen zij bij 221 incidenten gevolgen optreden in een andere infrastructuur. Er waren echter in totaal slechts zeven casus die een duidelijk verstorend effect hadden, waarbij de sectoren energie en

telecommunicatie veruit het vaakst de bron van het probleem waren. Verstoringen in andere sectoren (voeding, industrie, water, transport) leidden nooit tot een probleem in een andere sector. Niet geheel verrassend gaf een elektriciteitsuitval het vaakst aanleiding tot problemen in andere infrastructuren, maar grote gevolgen had het zelden. Door onder andere noodstroomvoorzieningen, maar ook vanwege bijvoorbeeld het feit dat operators bij gas en elektriciteit gebruikmaken van eigen telecommunicatie, bleven cascade-effecten zeer beperkt. Vergelijkbare resultaten leverden de vergelijking met de buitenlandse rapporten op. Cascades bleken veel uitzonderlijker dan gedacht en als ze zich een keer voordeden, reikten ze minder ver in andere sectoren dan verondersteld. Er is helaas geen recentere studie bekend naar cascade-effecten, ook niet specifiek voor cascade-effecten bij optreden klimaatrisico's, maar deze studie toont aan dat cascade-effecten veelal beperkt zijn, door voldoende weerbaarheid in vitale infrastructuur en noodcommunicatievoorzieningen. De afhankelijkheid van met name digitalisering in verschillende sectoren is verder toegenomen, met een grotere afhankelijkheid van elektriciteit en ICT, maar ook de aandacht voor weerbaarheid/redundantie binnen o.a. ICT.

Bij uitval van elektriciteit zijn noodstroomvoorzieningen noodzakelijk bijv. op de crisislocaties van crisispartners of knooppuntlocaties in de digitale infrastructuur. Bij uitval van telecommunicatie zijn er veelal alternatieven mogelijk voor OOV- en crisisorganisaties, zoals NCV, satellietcommunicatie of mobiele posten/voertuigen met communicatievoorzieningen en eigen stroomvoorziening via accu's of noodaggregaten. Voor de crisisorganisaties zijn er verschillende Nationale of Landelijke Crisisplannen (NCP/LCP), waaronder voor twee klimaatrisico's namelijk Natuurbranden [82] en Hoogwater en Overstromingen [83]. Daarnaast is ook het Nationaal Crisisplan Elektriciteit relevant, gelet op de cascade-effecten bij uitval van elektriciteit. Verder is er ook een Landelijk Crisisplan Digitaal [84] maar dit richt zich enkel op cyberaanvallen en -incidenten binnen de digitale infrastructuur, en niet op uitval door andere risico's zoals klimaatdreigingen. In het Landelijk Crisisplan Digitaal wordt wel onderkend dat de vitale processen in Nederland in toenemende mate afhankelijk zijn van gedigitaliseerde processen, de onderliggende (informatie)systemen en ketenafhankelijkheden. De Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV) geeft aan dat een vitale aanbieder altijd zelf verantwoordelijk blijft voor de eigen continuïteit en dienstverlening.

7.1.2.2 Landelijke crisisplannen

Hieronder is een analyse gedaan in hoeverre maatregelen tegen cascade-effecten bij uitval van ICT bij i) hoogwater en overstromingen, ii) natuurbranden en iii) uitval elektriciteit zijn opgenomen in de crisisplannen en of er hiervoor aanvullende maatregelen zijn beschreven.

7.1.2.2.1 Landelijk Crisisplan Hoogwater en Overstromingen

In het crisisplan zijn vijf oorzaken voor hoogwater en overstromingen onderkend. Naast natuurlijke oorzaken (hoogwater, al dan niet gecombineerd met andere scenario's als een hevige storm, hoge rivier afvoer, wateroverlast of springtij) zijn dit het falen van een kering, uitval van elektriciteit en telecommunicatie, opzettelijke manipulatie via internet (cyberaanval) en moedwillige verstoringen algemeen (terrorisme). De sector is voor de beweegbare keringen (inclusief sluizen en gemalen) afhankelijk van elektriciteit en de beschikbaarheid van telecommunicatie en ICT. Wanneer er langdurige verstoringen optreden op het gebied van elektriciteit of telecom, zullen de beweegbare keringen en gemalen veelal niet werken en dienen er noodmaatregelen te worden getroffen (bijv. handmatige bediening of

noodaggregaten). Hiermee zijn cascade-effecten ten gevolge van uitval van telecommunicatie en ICT indirect opgenomen, en zijn ook mogelijke noodmaatregelen beschreven.

7.1.2.2.2 *Landelijk Crisisplan Natuurbranden*

Bij een grootschalige natuurbrand kan vitale infrastructuur zoals (primaire) voorzieningen voor elektriciteit, drinkwater en telecommunicatie worden aangetast, wat op zichzelf weer tot nieuwe problemen kan leiden (cascade-effecten). Dit geldt niet alleen binnen het direct getroffen gebied, ook daarbuiten kan een deel van de vitale infrastructuur uitvallen. Mogelijke cascade-effecten zijn beschreven in het crisisplan, er zijn hierbij geen acute of preventieve maatregelen beschreven voor telecommunicatie.

7.1.2.2.3 *Nationaal Crisisplan Elektriciteit*

Er is ook een Nationaal Crisisplan Elektriciteit [85] uitgegeven door het Ministerie van Economische Zaken en Klimaat. Hierin zijn de overwegingen en het handelingsperspectief beschreven voor de overheid rondom:

- ☐ Communicatie richting burgers: Bij een grootschalige uitval van de elektriciteitsvoorziening zijn reguliere communicatiemiddelen zoals internet en tv al snel niet meer toegankelijk. Hierdoor is communicatie met de samenleving over de situatie en de hersteltijd al snel niet meer mogelijk via internet en TV. Het verminderd aantal middelen dat ingezet kan worden, beperkt de mogelijkheden van de overheid om te communiceren over het herstel en/of het verloop van de situatie. Mobiele masten raken binnen twee uur door hun accuduur (indien aanwezig) heen en vallen uit. Een eventuele NL-Alert met handelingsperspectief voor de bevolking moet in deze periode zijn verstuurd. Een mogelijke maatregel om communicatie met burgers nog wel mogelijk te maken, is gebruik maken van FM- en DAB-radio voor informeren via regionale crisiszender, waarnaar burgers bijvoorbeeld vanuit de auto of met een radio op batterijen kunnen luisteren. In de eerste twee uur kan hierin communicatieboodschappen (via NL Alert) naar gerefereerd worden. Dit vereist dat FM- en DAB-radio blijven werken bij een grootschalige uitval van de elektriciteitsvoorziening door middel van noodstroomvoorzieningen.
- ☐ Impact op crisisbeheersingsprocessen: Voor onderlinge informatie-uitwisseling tussen crisispartners wordt veel gebruik gemaakt van telecom en dataverkeer. Er is een landelijke NoodCommunicatieVoorziening (NCV). Het is afhankelijk van de noodstroomvoorziening van de betreffende actor/crisispartner hoelang het netwerk blijft functioneren. Hierdoor ontstaat een extra uitdaging in de crisisbeheersing als communicatie en informatie-uitwisseling binnen de landelijke crisissstructuur niet meer functioneert zoals eenieder gewend is. Indien de situatie dusdanig ernstig is dat nationale coördinatie c.q. landelijke regie niet meer mogelijk is, is gebruik maken van satellietcommunicatie toestaan (mits alle benodigde actoren die ook hebben) een mogelijkheid. Als alternatief voor communicatiemiddelen kunnen verschillende crisisteams koeriers inzetten of partners gaan fysiek naar crisiscentra. Daarnaast kan men inzet van radio zendamateurs (Dutch Amateur Radio Emergency Service, DARES) vragen, bijvoorbeeld op basis van een convenant met een veiligheidsregio.
- ☐ Omgaan met landelijke onbereikbaarheid hulpdiensten voor burgers via 112: Door uitval van elektriciteit valt met enkele uren de telecomvoorziening uit, waardoor ook 112 niet meer bereikbaar is. Hierdoor is onduidelijk waar hulpbehoevenden zijn en het volgen van hulpdiensten door een meldkamer is niet meer mogelijk. Politiebureaus, brandweer-ambulanceposten kan men bijv. continu bemensen als noodmeldpunt. Ook het verhogen van fysieke aanwezigheid op straat is een mogelijkheid door bijvoorbeeld meer te

surveilleren en inzet van extra handhavers. Een eventuele NL-Alert met handelingsperspectief voor de bevolking rondom 112 moet in deze periode zijn verstuurd.

7.1.3 Beleidsboodschap

De cascade-effecten bij uitval van elektriciteitsvoorziening en telecomnetwerken en het effect op openbare orde en veiligheid en acute hulpverlening zijn bekend. Voor de OOV- en crisisorganisaties zijn er specifieke (back-up) communicatienetwerken met verhoogde beschikbaarheid bij uitval elektriciteit, zoals C2000 (inclusief meldkamers), NCV, satelliettelefoons en DARES.

De besloten netwerken C2000 en NCV verschillen qua technische elementen niet wezenlijk van de digitale infrastructuur, zoals hierboven beschreven. De klimaatrisico's zijn voor deze besloten netwerken daarom niet wezenlijk anders. Het belangrijkste onderscheid is dat de overheid, via OOV- en crisisorganisaties, zelf verantwoordelijk is voor de weerbaarheid van deze besloten netwerken en zelf maatregelen moeten nemen om de risico's op uitval te beperken. Dit kan door voldoende redundantie in deze netwerken te gebruiken, door gebruik van terugval op alternatieven of door aanvullende maatregelen tegen (klimaat)risico's te nemen.

De beleidsboodschap is om de wettelijke maatregelen uit de Wet weerbaarheid kritieke entiteiten (Wwke) ook toe te passen op de sectorspecifieke digitale infrastructuur zoals C2000 en NCV, en hierin expliciet klimaatrisico's mee te nemen.

7.2 Elektriciteitsvoorziening

7.2.1 Digitale infrastructuur elektriciteitsvoorziening

De elektriciteitsvoorziening en -infrastructuur zijn essentieel voor Nederland. Vitale processen zijn afhankelijk van deze elektriciteitsvoorziening. Ook in niet vitale processen wordt de afhankelijkheid van de elektriciteitsvoorziening steeds groter. Dit betekent dat uitval van elektriciteit grote maatschappelijke gevolgen kan hebben, ook door de afhankelijkheid van de digitale infrastructuur van elektriciteit. De impact op verschillende vitale processen wordt veelal al binnen enkele uren merkbaar. Bij stroomuitval heeft men vanuit huis bijv. geen toegang meer tot internet, TV of radio via vaste aansluitingen (kabel, glasvezel), en na 2 tot 4 uur is ook het mobiele netwerk niet meer beschikbaar.

Binnen Nederland zijn landelijke en regionale netbeheerders verantwoordelijk voor elektriciteitsvoorziening en -infrastructuur. In deze paragraaf richten we ons op de vitale ICT-systemen en applicaties binnen netbeheerders, die cruciaal zijn voor telecommunicatie bij herstel van stroomuitval. We richten ons niet op de uitval door (klimaat)risico's van de elektriciteitsnetwerken zelf en de IT-componenten voor monitoring en beheer van deze netwerken. Deze analyse is binnen een andere deelstudie uitgevoerd voor PBL door de TU Delft.

Netbeheerders zijn wettelijk verplicht om te zorgen voor robuuste communicatie en applicaties via artikel 41 (Communicatiesystemen) van de Verordening (EU) 2017/2196 en artikel 24 van de Verordening (EU) 2017/1485. Hierin is vastgelegd dat netbeheerders in

transmissie en distributienetwerken over communicatievoorzieningen moeten beschikken voor informatievoorziening tussen overheid en netbeheerders die blijven werken bij een black-out:

... elke aanbieder van hersteldiensten en elke transmissiesysteembeheerder (TSB) voert een spraakcommunicatiesysteem in met voldoende reserveapparatuur en back-upvermogensbronnen zodat ten minste 24 uur lang informatie over het herstelplan kan worden uitgewisseld indien de externe elektriciteitsvoorziening volledig uitvalt of de afzonderlijke apparatuur van het spraakcommunicatiesysteem defect is. De lidstaten kunnen eisen dat de minimale reservecapaciteit langer dan 24 uur kan worden benut.

Netbeheerders zoals TenneT hebben invulling gegeven aan deze wettelijke eisen rondom systeembescherming en herstel [86], met een beschrijving van procedures en de te gebruiken telecommunicatie-infrastructuur [87]. Deze telecommunicatie-infrastructuur bestaat uit:

- Publieke communicatie-infrastructuur: Onder normale omstandigheden is de publieke communicatie-infrastructuur voldoende om alle partijen te bereiken, maar onder storingssituaties in de publieke communicatie-infrastructuur of bij black-out kan niet gegarandeerd worden dat de communicatie gehandhaafd blijft.
- Satelliettelefonie: In geval van falen van de publieke communicatie-infrastructuur kan satelliettelefonie worden toegepast als terugval scenario voor de spraakcommunicatie.
- Private communicatie-infrastructuur: spraak/data communicatie-infrastructuur van TenneT is uitgerust met noodvoeding om een hoge mate van betrouwbaarheid en beschikbaarheid te hebben.

Deze infrastructuren kunnen worden gebruikt in geval van uitval van stroomvoorziening en/of telecommunicatie, ook bij klimaatrisico's. Binnen de landelijke en regionale netbeheerders zijn ook noodstroomvoorzieningen aanwezig voor vitale ICT-systemen en applicaties en voor interne telecommunicatie.

7.2.2 Klimaatrisico's sectorspecifieke infrastructuur

Bovenstaande netwerken verschillen qua technische elementen niet wezenlijk van de digitale infrastructuur zoals beschreven in hoofdstuk 3. Er zijn verschillende back-up voorzieningen, waarbij noodstroomvoorzieningen een belangrijke component vormen voor continuïteit bij stroomuitval van de private communicatie-infrastructuur en satelliettelefonie.

Daarnaast is er een Nationaal Crisisplan Elektriciteit. Hierin is beschreven welke overheidsorganisaties een rol hebben in de crisisstructuur samen met de landelijke (TenneT) en regionale netbeheerders. Het crisisplan beschrijft de inhoudelijke stappen die bij de beheersing van elektriciteitscrisis gezet moeten worden t.a.v. bronbestrijding en gevolgbestrijding. Voor de OOV-sector is dit beschreven in

7.2.3 Beleidsboodschap

Netbeheerders zijn wettelijk verplicht om te zorgen voor robuuste communicatie en applicaties voor informatievoorziening tussen overheid en netbeheerders die blijven werken bij een black-out en herstel. TenneT en andere netbeheerders hebben invulling gegeven aan deze wettelijke eisen rondom systeembescherming en herstel [86], met een beschrijving van procedures en de te gebruiken telecommunicatie-infrastructuur [87]. Deze telecommunicatie-

infrastructuur bestaat uit publieke communicatie-infrastructuur, satelliettelefonie en private communicatie-infrastructuur.

Deze infrastructuren kunnen worden gebruikt in geval van uitval van stroomvoorziening en/of telecommunicatie, ook ten gevolge van klimaatrisico's. Er is door TNO geen nadere analyse uitgevoerd in hoeverre de private communicatie-infrastructuur van netbeheerders en satellietcommunicatie bestand zijn tegen de verschillende klimaatrisico's.

De beleidsboodschap is om de wettelijke maatregelen uit bijv. de Wet weerbaarheid kritieke entiteiten (Wwke) ook toe te passen op de sectorspecifieke digitale infrastructuur en hierin expliciet klimaatrisico's mee te nemen die leiden tot gelijktijdige uitval van de elektriciteitsvoorziening en de private digitale infrastructuur.

7.3 Gezondheidszorg

7.3.1 Digitale infrastructuur gezondheidszorg

De fysieke ICT-infrastructuur binnen de Nederlandse gezondheidszorg omvat alle hardware, netwerken en faciliteiten die nodig zijn om digitale zorgprocessen te ondersteunen. Dat bestaat uit datacenters en serverruimtes, netwerkinfrastructuur en hardwarecomponenten. Binnen de gezondheidszorg vindt, net als in andere sectoren, steeds meer transformatie plaats naar hybride cloud modellen (met privaat én publieke cloud), al blijft de fysieke ICT-infrastructuur in ziekenhuizen zelf cruciaal voor sommige toepassingen zoals radiologie.

De NEN 7510 [88] is een norm waaraan voldaan moet worden en is ten behoeve van informatiebeveiliging in de zorg. Ook moeten zorginstellingen sinds 2018 voldoen aan de eerste Europese NIS-richtlijn, via de Wet beveiliging netwerk- en informatiesystemen (Wbni). De nieuwe NIS2-richtlijn (opvolger van NIS) wordt in Nederland naar verwachting in het tweede kwartaal van 2026 van kracht via de Cyberbeveiligingswet (Cbw). De zorgsector is onderdeel van de vitale infrastructuur, wat strengere eisen stelt aan fysieke en digitale weerbaarheid [89].

Dit hoofdstuk behandelt de risico's die samenhangen met klimaatverandering voor de ICT in de zorgsector. Het hoofdstuk richt zich specifiek op Nederlandse ziekenhuizen, gebaseerd op gesprekken met vijf experts werkzaam bij verschillende ziekenhuizen in Nederland.

7.3.2 Klimaatrisico's sectorspecifieke infrastructuur

7.3.2.1 Crisisplannen en Oefeningen

Ziekenhuizen zijn zelf verantwoordelijk voor het opstellen en uitvoeren van crisisplannen, waaronder het Ziekenhuis Rampen Opvang Plan (ZiROP). In deze plannen worden ook scenario's geoefend die gerelateerd zijn aan klimaatverandering. De nadruk ligt op het organiseren van crisisteams en het uitwerken van rampen- en crisismanagementplannen tot in detail. Kennisoverdracht vindt plaats via samenvattingen en vooral door het houden van oefeningen, zodat medewerkers weten wat van hen wordt verwacht.

7.3.2.2 ICT-infrastructuur en datacenters

Netwerken, opslag, bekabeling en datacenters vormen de ruggengraat van de ICT binnen ziekenhuizen. Dit ICT-fundament ondersteunt vrijwel alle zorgprocessen; uitval van zo'n kerncomponent raakt meerdere serviceketens tegelijk. Een opvallende trend is de toenemende uitbesteding van ICT-diensten aan ICT-aanbieders via externe datacenters, wat de afhankelijkheid van de bredere ICT-sector vergroot. Binnen deze infrastructuur zijn componenten als centrale opslag en integratieplatformen van vitaal belang; uitval van deze onderdelen raakt direct meerdere zorgprocessen, wat de impact van storingen extra groot maakt.

In veel ziekenhuizen bevindt de ICT-infrastructuur zich fysiek op de begane grond, in de kelder of het souterrain. Deze locaties maken de systemen bijzonder kwetsbaar voor overstromingen. Om de continuïteit te borgen is er doorgaans sprake van redundantie: ziekenhuizen beschikken vaak over twee datacenters die onafhankelijk van elkaar kunnen functioneren. Toch staan ook deze redundante datacenters veelal op de begane grond, waardoor de kwetsbaarheid blijft bestaan. Een illustratief praktijkvoorbeeld betreft het overstromingsincident bij het VUMC in 2015, veroorzaakt door een kapotte waterleiding. De schade en verstoring die toen ontstonden, zijn vergelijkbaar met de gevolgen van overstromingen door klimaatverandering.

Het verplaatsen van kritieke ICT-systemen van het ziekenhuis-souterrain naar een professioneel colocatie-datacenter of naar de cloud vermindert doorgaans de blootstelling aan klimaatrisico's zoals overstromingen en hitte, en verhoogt de basisweerbaarheid. Colocatie- en cloudlocaties zijn vaak beter beschermd dankzij professionele facility-hardening: ze bieden hoger gelegen en gecompartmenteerde datavloeren, waterkerende voorzieningen en lekdetectie, betrouwbare stroom- en koelvoorzieningen en 24/7 monitoring. Deze maatregelen zijn doorgaans beter geregeld dan in een gemiddelde ziekenhuisservruimte.

Het voordeel van deze migratie is echter afhankelijk van een zorgvuldig ontworpen architectuur. Hoewel het fysieke risicoprofiel door verplaatsing afneemt, ontstaat er een nieuwe afhankelijkheid van ketens en leveranciers. Denk hierbij aan kwetsbaarheden in netwerkverbindingen, regionale incidenten of storingen in cloudregio's. Het is dus van belang om bij de inrichting van alternatieve locaties niet alleen te letten op facility-hardening, maar ook op de nieuwe vormen van afhankelijkheid die ontstaan.

7.3.2.3 Medische apparatuur

Bij medische apparatuur kan gedacht worden aan MRI- en CT-scanners, infuuspompen en OK-apparatuur. Deze apparaten zijn doorgaans in eigen beheer vanwege hun kritische rol. Medische apparatuur is steeds afhankelijker van dit fundament; bij uitval is alleen een beperkte *stand alone* modus mogelijk.

De klimaatgerelateerde risico's die specifiek op deze medische apparatuur werken zijn echter gering omdat deze systemen zich binnen het gebouw bevinden. Ernstige schade aan deze systemen door stormen of overstromingen zou duiden op veel grotere problemen voor het ziekenhuis als geheel.

7.3.2.4 Facilitaire infrastructuur (elektriciteitsvoorziening en koeling)

Elektriciteit is vooral kwetsbaar voor overstromingen. Ziekenhuizen beschikken over noodstroomvoorzieningen die regelmatig getest worden. Door bezuinigingen ontbreekt het in sommige gevallen aan eigen experts op dit gebied, waardoor kennis vaak wordt uitbesteed. Meerdere ziekenhuizen geven aan op relatief regelmatige basis te maken te hebben met (beperkte) stroomstoringen en het testen van de noodstroomvoorziening. Hierin vindt ook altijd een automatische fasering plaats: eerst worden de niet-kritische processen uitgeschakeld.

De koelketen raakt overbelast bij hittegolven en tropennachten. Faalt de koeling, dan grijpen systemen thermisch in (noodstop of kloksnelheid omlaag), met uitval tot gevolg. Praktijkvoorbeelden, zoals de problemen bij de NHS in het Verenigd Koninkrijk tijdens een hittegolf in 2022, tonen aan dat langdurige zorg-ICT-verstoring kan optreden na koeluitval in datacenters [90].

7.3.2.5 Primaire zorgsystemen

Systemen zoals het Elektronisch Patiëntendossier (EPD), PACS (beeldarchivering) en medicatiebewaking zijn meestal binnen een ziekenhuis (on-premise) of in colocatie, vooral vanwege eisen op het gebied van privacy en continuïteit. Op deze primaire zorgsystemen zijn losse klimaatrisico's nauwelijks van toepassing. Deze systemen zijn echter wel sterk afhankelijk van elektriciteitsvoorzieningen en netwerkconnectiviteit, en kunnen als cascade-effect dus wel kwetsbaar zijn.

7.3.2.6 Netwerkconnectiviteit

Netwerksegmentatie, firewalls, monitoring en incident response worden doorgaans intern beheerd, vanwege de strikte eisen rond informatiebeveiliging en compliance met NEN7510. Het inzien van patiëntgegevens en het delen van deze gegevens met andere zorginstellingen is in toenemende mate afhankelijk van connectiviteit. Beelden in radiologie worden in toenemende mate geanalyseerd met (AI-)software. In een scenario van lange stroomuitval is het mogelijk dat deze diensten volledig wegvallen en moeilijk op te lossen zijn. Antennes en andere hardware is mogelijk kwetsbaar voor extreme weersomstandigheden, omdat deze zich typisch in en rondom de buitenste schil van de gebouwen bevindt. Betrokkenen geven echter aan dat er momenteel weinig incidenten zijn op het gebied van stormschade, en zich weinig zorgen maken dat zwaardere stormen voor grote problemen zullen zorgen.

7.3.3 Beleidsboodschap

Kerninzichten uit de interviews

- ☐ Initiatieven om klimaatrisico's te beheersen komen vooral van ziekenhuizen zelf. Er is een overkoepelend orgaan voor kennisuitwisseling, maar geen breed geaccepteerd framework voor klimaatgerelateerde ICT-risico's.
- ☐ Er bestaan algemenere risico-inventarisatiemethodes, maar deze besteden geen specifieke aandacht aan klimaatrisico's.
- ☐ De infrastructuur en interne datacenters zijn met name kwetsbaar voor neerslag en overstromingen, omdat ze vaak op de begane grond of in souterrains zijn gesitueerd. Het programma "weerbare zorg" van het ministerie van VWS wordt momenteel uitgevoerd, in samenhang met de Wet weerbaarheid kritieke entiteiten (Wwke). Vooral specialistische academische ziekenhuizen verwachten binnen het bereik van deze wet te vallen vanwege

hun essentiële rol binnen acute ziekenhuiszorg en spoedeisende hulp. In dit kader worden stuurgroepen en projectgroepen opgericht die zich richten op het vergroten van de weerbaarheid. Ook de Cyberbeveiligingswet (gebaseerd op de Europese richtlijn NIS2) geldt voor ziekenhuizen. Deze regelgeving vereist een gedegen organisatie van personeel, locatie, IT en crisismanagement.

Binnen ZiROP werken ziekenhuizen nauw samen met overheden en andere zorginstellingen. Daarnaast streeft men naar het behalen van relevante medische en informatiebeveiligingscertificeringen, hetgeen onder meer regelmatig oefenen en het delen van informatie met medewerkers vereist.

Sectorbreed beleid is hoofdzakelijk gericht op algemene ICT-uitval; specifiek beleid ten aanzien van klimaatverandering bevindt zich nog in een beginstadium. De focus ligt voornamelijk op het beheersen van stroomuitval, terwijl aandacht voor het mitigeren van klimaateffecten beperkt blijft.

De overheid biedt richtlijnen voor continuïteit en beveiliging van zorg-ICT, maar stelt tot op heden weinig concrete eisen met betrekking tot het adresseren van klimaatrisico's. Ziekenhuizen zijn zelf verantwoordelijk voor het inschatten van risico's en het treffen van passende maatregelen. Betrokken partijen geven aan behoefte te hebben aan meer duidelijke handreikingen vanuit de overheid, onder meer ter bevordering van landelijke uniformiteit en kennisdeling. Dit kan ziekenhuisorganisaties ondersteunen bij het stellen van prioriteiten rondom benodigde maatregelen.

Geïnterviewden benadrukken de noodzaak van aanvullende middelen en richtlijnen vanuit de overheid, met name van het ministerie van VWS. Er bestaat een wens voor heldere minimumnormen met betrekking tot risicobeoordelingen, scenario's en beheersmaatregelen, waarbij tevens ruimte dient te blijven bestaan voor eigen invulling door ziekenhuizen.

7.4 Transport

7.4.1 Digitale infrastructuur transport

De fysieke ICT-infrastructuur in de transportsector is cruciaal voor het functioneren van logistiek, mobiliteit en veiligheid. De transportsector omvat wegvervoer, spoorvervoer, binnenvaart, zeevaart en luchtvracht. Luchttransport en de zeevaart heeft een relatief centraal karakter, met vliegvelden en grote havens als belangrijke knooppunten. Wegvervoer, spoorvervoer en binnenvaart hebben daarentegen een sterk gespreid karakter.

Vanwege beperkte tijd is dit onderzoek beperkt geweest tot het spoorvervoer middels een interview met ProRail. Wij verwachten dat de hieruit voortgekomen resultaten over het algemeen te generaliseren zijn naar wegvervoer en binnenvaart: de infrastructuur van deze sectoren is eveneens in (semi-)publiek eigendom bij een relatief gedecentraliseerde organisatie. Rondom luchttransport en zeevaart is het moeilijker om conclusies te trekken.

Binnen het spoortransport worden drie lagen van ICT onderscheiden, ieder met een eigen rol en risicoprofiel. De eerste laag bevat de systemen die direct nodig zijn om treinen te laten rijden, zoals planningssystemen, aansturingsoftware en systemen voor realtime bijsturing.

Het landschap bestaat uit veel legacy-toepassingen die draaien op specifieke, vaak verouderde hardware, waarvan delen nog fysiek op locatie staan. Deze systemen zijn missiekritisch: uitval kan direct gevolgen hebben voor de veiligheid, beschikbaarheid en punctualiteit van het treinverkeer. Modernisering is complex door de hoge mate van verwevenheid met bestaande processen en infrastructuur.

De tweede laag ondersteunt het beheer van alle fysieke spoorassets, zoals wissels, seinen, kunstwerken en voorzieningen langs het spoor. Naast registratieve systemen voor onderhoud en vervanging groeit de mate van IT/OT-integratie snel. Sensoren meten continu de status van infrastructuur, zoals slijtage van wissels, temperatuur van apparatuur of de werking van ventilatie- en brandbeveiligingsinstallaties. Deze 'slimmere' systemen vergroten de voorspelbaarheid en efficiëntie van onderhoud, maar brengen ook nieuwe risico's met zich mee, onder andere op het gebied van cybersecurity, datakwaliteit en de robuustheid van systemen bij extreme weersomstandigheden of andere klimaatgerelateerde effecten.

De derde laag omvat de algemene bedrijfsvoering, waaronder administratieve processen, logistiek ondersteunende systemen en de vele SaaS-oplossingen die worden afgenomen bij externe leveranciers. Voor assetmanagement worden daarnaast standaardapplicaties gebruikt die zijn afgestemd op de omgeving van ProRail. Vooral binnen de logistieke processen is nog veel sprake van maatwerksystemen die nauw aansluiten op het operationele domein. Deze laag is minder *mission critical* dan de twee onderliggende lagen, maar vormt wel de ruggengraat voor efficiënte bedrijfsvoering en verantwoording.

Daarnaast beschikt ProRail over een eigen GSM-netwerk (GSM-R) dat specifiek is ingericht voor communicatie en beveiliging binnen het spoorvervoer. Dit netwerk wordt onder andere gebruikt voor de communicatie met treinen en het waarborgen van de veiligheid op het spoortraject. Het beheer van dit netwerk is wettelijk verplicht en wordt uitgevoerd door een interne telecomafdeling. Bovendien zal het nieuwe Europese beveiligingssysteem hierop aansluiten. De operationele uitvoering van het netwerk is uitbesteed aan een externe partij, in dit geval Nokia.

7.4.2 Klimatrisico's sectorspecifieke infrastructuur

ProRail onderkent dat klimaatverandering een toenemend strategisch risico vormt voor het spoor. De spoorinfrastructuur bevindt zich grotendeels in de buitenruimte en is daardoor direct kwetsbaar voor veranderende klimatologische omstandigheden, waaronder hevige regenval, hitte en stormschade. Hoewel binnen de organisatie aan dit onderwerp wordt gewerkt, richt de aandacht zich momenteel vooral op cyberdreigingen, sabotage en risico's rond stroomuitval. De mogelijke invloed van klimaatverandering op de IT-infrastructuur is hierdoor nog niet volledig geïntegreerd in de reguliere risicobeoordeling.

7.4.2.1 Risicobeoordeling van ICT-componenten

Voor ICT-componenten en de processen waarin zij samenwerken worden risicoclassificaties uitgevoerd. Netwerken worden hierbij vrijwel standaard als missiekritisch aangemerkt. De gedecentraliseerde inrichting van zowel het spoornetwerk als de ICT-architectuur zorgt er doorgaans voor dat defecten in componenten slechts leiden tot lokale verstoringen. Door de toenemende intensiteit, compactheid en efficiëntie van het Nederlandse spoorstelsel

veroorzaken dergelijke lokale storingen echter steeds vaker cascade-effecten die ook elders in het land leiden tot vertragingen of uitval.

7.4.2.2 Versterking van systeemweerbaarheid

Om de weerbaarheid van het systeem te vergroten ontwikkelt ProRail een architectuur waarin drie geografisch gescheiden ICT-knooppunten continu gesynchroniseerd zijn. Elk knooppunt moet zelfstandig in staat zijn om op elk moment de landelijke aansturing over te nemen. Deze inrichting ondersteunt toekomstig locatie-onafhankelijk werken en minimaliseert de gevolgen van verstoringen, ongeacht hun oorsprong. Het streven is te komen tot twee of drie identieke datacenters die elkaars functionaliteit volledig kunnen opvangen.

7.4.2.3 Kwetsbaarheid en redundantie van verkeersleidingsposten

De huidige datacenters op de dertien verkeersleidingsposten zijn relatief kwetsbaar door hun ligging op of onder maaiveldniveau, waardoor zij risico lopen bij hevige neerslag en overstromingen. Om deze kwetsbaarheid te mitigeren beschikt iedere post over een colocatie in een andere regio, die de functionaliteit kan overnemen. Deze opstellingen worden periodiek getest en kunnen indien nodig preventief worden geactiveerd. Een voorbeeld hiervan vormt de overstromingssituatie in Limburg in 2021, waarbij uit voorzorg is overgeschakeld naar de uitwijklocatie van de verkeersleidingspost Maastricht.

7.4.2.4 Operationele praktijk en leervermogen

Uit incidentanalyses blijkt dat het overgrote deel van verstoringen binnen het spoor wordt veroorzaakt door menselijk handelen. De sector is gewend om frequent met lokale storingen om te gaan, die zelden levensbedreigend zijn en onderdeel vormen van de dagelijkse operatie. Dit zorgt voor een goed geoefende crisisorganisatie met sterke routine in het beheersen en herstellen van incidenten.

7.4.2.5 Levensduur en klimaatbestendigheid van ICT-componenten

Veel ICT-componenten die zich buiten bevinden kennen een relatief korte technische levensduur van enkele jaren. Hierdoor kunnen klimaatgerelateerde risico's, zoals extreme hitte, droogte of neerslag, vaak binnen reguliere vervangingscycli worden ondervangen. Indien bepaalde componenten sneller verouderen of vaker uitval vertonen door veranderende omstandigheden, kan bij vervanging worden gekozen voor een robuustere variant.

De ICT-onderdelen met de langste levensduur zijn die bij bruggen, tunnels en viaducten. Bij het (her-)plaatsen van dergelijke componenten is het van belang een langere tijdshorizon aan te houden en mogelijke klimaatgerelateerde risico's nadrukkelijk mee te wegen in ontwerpkeuzes en locatiebepaling.

7.4.3 Beleidsboodschap

De spoortransportsector beschikt over een goed ingerichte en ervaren crisisorganisatie, die dagelijks te maken heeft met uiteenlopende verstoringen. Door de modulaire en gedecentraliseerde opbouw van het spoorstelsel leidt een incident doorgaans tot uitsluitend lokale uitval. Hierdoor blijft de directe impact van lokale klimaatgerelateerde risico's op dit moment relatief beperkt.

Voor nieuwe objecten en ICT-componenten met een lange levensduur geldt echter dat toekomstige klimaatverandering nadrukkelijker moet worden meegewogen in ontwerp-, locatie- en investeringsbeslissingen. Dit voorkomt dat nu geplaatste systemen in de toekomst kwetsbaar blijken voor extremere neerslag, hogere temperaturen of andere klimaatgerelateerde risico's.

ProRail geeft aan dat de sector behoefte heeft aan meer duidelijkheid en richting vanuit de overheid ten aanzien van verwachte klimaatontwikkelingen en de bijbehorende handelingsperspectieven. De huidige onzekerheden over het te verwachten verloop van klimaatverandering maken het lastig om te bepalen welke maatregelen noodzakelijk, proportioneel en toekomstbestendig zijn. Heldere nationale kaders, scenario's en richtlijnen zouden de sector ondersteunen bij het tijdig en doelgericht aanpassen van infrastructuur en ICT-systemen, zodat de spoorsector blijvend veilig en robuust kan functioneren in een veranderend klimaat.

8 Reflecties en conclusies

8.1.1 Wat leren we over klimaatrisico's voor de digitale infrastructuur?

Risicobeeld bij huidig beleid: laag tot 2050, maar niet nul

De analyses in de voorgaande hoofdstukken laten zien dat het restrisico voor de digitale infrastructuur tot 2050 in het algemeen beperkt blijft wanneer het huidige beleid wordt doorgezet en gangbare redundantiemaatregelen op orde zijn. Dat betekent niet dat het risico verdwijnt. De kwetsbaarheid neemt vooral toe bij zeldzame maar zwaardere scenario's, zoals regionale stroomuitval, extreme neerslag of een combinatie van langdurige hitte met waterschaarste. In die situaties kunnen verstoringen in elektriciteitsvoorziening, telecommunicatie en datacenters elkaar snel versterken.

De blootstelling is niet overal gelijk. Datacenters en netwerkpunten in gebieden met een hogere kans op overstroming of wateroverlast zijn gevoeliger voor fysieke schade en uitval. De sterke concentratie van colocatiecapaciteit in de Metropoolregio Amsterdam vergroot bovendien de kans op systeemeffecten bij regionale incidenten. Spreiding over meerdere clusters, bij voorkeur in gebieden met lagere watterisico's en voldoende energie- en netwerkcapaciteit, vermindert die systeemkwetsbaarheid.

De kwetsbaarheid wordt in hoge mate bepaald door technische en organisatorische keuzes. Koelsystemen die voldoende presteren bij hoge buitentemperaturen en tropische nachten, elektrische installaties met dubbele voedingen, en een doordachte plaatsing van kritieke componenten boven maatgevende waterlijnen verlagen de kans op uitval. Voor de continuïteit is verder van belang dat uitwijklocaties echt onafhankelijk zijn: niet in hetzelfde overstromingsbekken, niet op dezelfde elektrische netstations aangesloten en via fysiek gescheiden glasvezelroutes bereikbaar.

De ketenafhankelijkheden blijven de belangrijkste risicofactor voor de maatschappelijke impact. De meeste digitale diensten vallen niet uit door één enkel knelpunt, maar doordat meerdere schakels tegelijk worden geraakt. Regionale of nationale stroomstoringen, beperkingen in telecommunicatie of verstoringen bij cloud- en datacenterdiensten kunnen elkaar in korte tijd beïnvloeden. Het is daarom nodig om niet alleen de individuele assets te versterken, maar ook de afspraken voor herstel en prioritering in de keten helder te organiseren.

Waar zit de blootstelling en kwetsbaarheid?

- ☐ **Masten/opstelpunten** zijn vooral gevoelig voor hitte (koeling/elektronica) en extreem weer (storm, natte sneeuw, bliksem). Reductie van uitval volgt uit technische hardening en redundantie in backhaul/voeding (N+1 of hoger).
- ☐ **Datacenters** kennen een gecombineerd risico bij hitte bij langdurige droogte (koellast neemt toe door hitte, eventuele beperkingen op koelwater bij langdurige droogte) en een

locatieafhankelijk risico bij wateroverlast/overstroming. Risicoreductie volgt uit bronkeuze voor koelwater, WUE-normering, bouwkundige maatregelen (drempels, opstelhoogte) en geografische scheiding van uitwijklocaties in andere regio's binnen Nederland of binnen Europa.

- **Netwerk/keten:** het dominante indirecte risico blijft stroomuitval. De grootste impact ontstaat bij keteneffecten (elektriciteit → telecom → cloud/datacenters). Vermindering vraagt geografische scheiding (primaair/uitwijk niet in hetzelfde overstromingsbekken of elektriciteitsnet), meervoudige energie (A/B-feed + bewezen noodstroom), netwerk/cloud-diversiteit (twee providers, fysiek gescheiden routes, meerdere regio's) en afspraken over prioritaire storingsherstel en periodieke testen van het automatische overschakelen naar een back-up- of reservesysteem (failover testen).

Systeemeffecten vragen spreiding en standaardisering

De huidige concentratie van colocatiecapaciteit in de MRA (>70%) vergroot de systeem-kwetsbaarheid bij regionale incidenten. Een tweede nationaal cluster en duidelijke toetsingscriteria (laag overstromingsrisico, niet-drinkwater voor koeling, dubbele energie/WAN) verlagen het restrisico voor Nederland als geheel.

Sectorspecifiek (H7): afhankelijkheden zijn doorslaggevend

Zorg, energie, OOV en transport leunen op dezelfde generieke digitale infrastructuur, met daarnaast eigen ICT-infrastructuur. De sterkte van de generieke digitale infrastructuur zit in professionaliteit en redundantie bij de grotere aanbieders; de zwakte van sectorspecifieke infrastructuur treedt op bij versnipperde ICT-systemen en (beheer)organisatie en bij single-tenant faciliteiten met beperkte (oefening met) uitwijkvoorzieningen. Migratie naar colocatie/cloud kan de fysieke kwetsbaarheid reduceren, mits contractueel geborgd (continuïteit en hersteltijden bij calamiteiten, multi-region architecturen, fysieke locaties niet in hetzelfde overstromingsgebied).

8.1.2 Wat betekent dit voor beleid en uitvoering?

Het huidige beleid neemt een belangrijk deel van de klimaatrisico's al weg, maar de mate waarin maatregelen daadwerkelijk worden toegepast en geborgd, bepaalt het uiteindelijke effect. In de praktijk gaat het om twee samenhangende lijnen: keuzes over waar digitale infrastructuur wordt toegestaan of uitgebreid, en keuzes over hoe die infrastructuur technisch en organisatorisch wordt ingericht. Daarnaast speelt de vraag hoe afspraken in de keten en de monitoring van prestaties worden vastgelegd.

Ruimtelijke richting (transformeren)

De blootstelling van het systeem neemt af wanneer nieuwe of uitbreidende datacenters worden gesitueerd op locaties met een lage kans op overstroming en wateroverlast. De huidige concentratie van colocatiecapaciteit rond de MRA vergroot de impact van regionale gebeurtenissen. Een tweede nationaal cluster, of een evenwichtiger groei van bestaande kleinere clusters, vergroot de veerkracht van het geheel. Bij locatiekeuzes ligt het voor de hand om randvoorwaarden vooraf mee te nemen: water-positieve voorzieningen zoals regenwateropvang en buffering, aantoonbare toegang tot duurzame energiebronnen, en toegang tot meerdere glasvezelnetwerken (aanbieders, routes, etc.).

Techniek en operatie (intensiveren)

De kwetsbaarheid van faciliteiten hangt samen met de inrichting van koeling, stroomvoorziening en de fysieke positionering van kritieke componenten. Systemen die blijven presteren bij

hogere buitentemperaturen en tropische nachten verkleinen de kans op uitval. Het plaatsen van elektrische en ICT-voorzieningen boven maatgevende waterlijnen beperkt schade bij lokale waterstanden. Afhankelijkheid van drinkwater kan in warme, droge perioden knellen; alternatieve bronnen zoals regenwater, industriewater of gezuiverd oppervlaktewater verminderen dit risico. Prestatie-indicatoren zoals WUE voor watergebruik en PUE voor energie maken efficiëntie en naleving inzichtelijk.

Ketenafspraken en monitoring

De grootste maatschappelijke effecten ontstaan wanneer verstoringen elkaar in de keten versterken. Regionale afspraken over prioriteit bij het herstel van digitale knooppunten en data-centerclusters verkorten de uitvalduur. In de implementatie van de Wwke en Cbw voor zowel vitale aanbieders binnen de digitale infrastructuur als voor vitale aanbieders in sectoren zoals elektriciteit, OOV, zorg en transport ontstaat ruimte om klimaatrelevante risico's, expliciet en toetsbaar op te nemen in risicobeoordelingen. Een compacte set indicatoren, onder meer locatiehoogte ten opzichte van NAP, herkomst van koelwater, resultaten van tests met noodstroom en koeling, en mate van geografische scheiding tussen primaire en uitwijklocaties, maakt voortgang zichtbaar en ondersteunt gerichte bijsturing.

In samenhang bezien leidt deze benadering tot een stapsgewijze daling van het restrisico. Keuzes over ligging en spreiding verminderen de blootstelling van het systeem, technische en organisatorische eisen verkleinen de kwetsbaarheid, en afspraken in de keten verkorten de hersteltijd tijdens zwaardere scenario's.

Interviewlijst

Interview met	Datum
ANVS	13-9-2024
Bytesnet (datacenter)	16-12-2024
Deltares	15-8-2024
DGWB	13-8-2024
Dialogic (datacenter)	17-7-2024
HMC (ziekenhuis)	14-8-2024
ProRail	9-10-2024
Rijkswaterstaat	21-8-2024
Schiphol	27-8-2024
TNO expert robuustheid kritieke ICT systemen	18-7-2024
TNO expert 5G en 6G	12-6-2024
TNO expert digitale netwerken	28-6-2024
TNO expert duurzaamheid ICT	15-4-2024
TNO expert telecom wetgeving	10-4-2024
TNO expert innovatie ICT	15-4-2024
TNO expert bereikbaarheid nooddiensten	25-6-2024
TNO expert vitale infrastructuur	15-8-2024
TNO expert toekomstige digitale infrastructuur	6-5-2024
TNO expert digitale netwerken	6-5-2024
Transport en Logistiek Nederland	15-8-2024
Veiligheidsregio Utrecht	3-9-2024
Nederlandse telecomoperator	1-4-2025
Ministerie van EZ - vitaal	26-2-2025
Ministerie van EZ - datacenters	11-5-2025
Amsterdam UMC	31-10-2025
Diakonessenhuis	12-11-2025
Erasmus MC	19-11-2025
Radboudumc	10-12-2025
St. Antonius Ziekenhuis	11-12-2025
ProRail	13-1-2026

Afkortingen

Afkorting Betekenis

AI	Artificial Intelligence
BBL	Besluit Bouwwerken Leefomgeving
BBP	Bruto Binnenlands Product
CBS	Centraal Bureau voor de Statistiek
Cbw	Cyberbeveiligingswet
Cbw	Cyberbeveiligingswet
CCAP	Climate Change Adaptation Plan
CCS	Carbon Capture and Storage
CER	Critical Entities Resilience
CIS	Cloud Infrastructure and Servicest
CNDCP	Climate Neutral Data Centre Pact
DAB	Digital Audio Broadcasting
DAS	Distributed Antenna System
DDCA	Dutch Data Center Association
DMA	Digital Market Act
DNS	Domain Name Service
DSA	Digital Services Act
DVB	Digital Video Broadcasting
EECC	European Electronic Communications Code
EMEA	Europe Middle East & Africa
EZ	Economische Zaken
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICT	Informatie en Communicatie Technologie
IPCC	Intergovernmental Panel on Climate Change
IPCEI	Important Projects Common European Interest
ISO	International Standardization for Organization
KNMI	Koninklijk Nederlands Meteorologisch Instituut
LCP	Landelijk Crisisplan
LIWO	Landelijk Informatiesysteem Water en Overstromingen
MRA	Metropool Regio Amsterdam
NAP	Normaal Amsterdams Peil
NAS	Nationale klimaatAdaptatieStrategie
NCP	Nationale Crisisplan
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCV	NoodCommunicatieVoorziening

NIPV	Nederlands Instituut Publieke Veiligheid
NIS/NIS2	Network and Information Security
ODC	Overheidsdatacenter
OOV	Openbare Orde en Veiligheid
OT	Operational Technology
PBL	Planbureau van de Leefomgeving
PUE	Power User Efficiency
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
TCFD	Task Force on Climate-related Financial Disclosures
TETRA	Terrestrial Trunked Radio
Tw	Telecommunicatiewet
WLO	Welvaart en Leefomgeving
WUE	Water Usage Efficiency
Wwke	Wet weerbaarheid kritieke entiteiten

Referenties

- [1] Planbureau voor de leefomgeving (PBL), „Aanpassen aan klimaatverandering – Kwetsbaarheden zien, kansen grijpen, Den Haag,” 2015.
- [2] Planbureau voor de leefomgeving (PBL), „Van risicobeoordeling naar adaptatiestrategie,” 2015.
- [3] Planbureau voor de leefomgeving (PBL), „ Wereldwijde klimaateffecten - Risico's en kansen voor Nederland, Den Haag,” 2015.
- [4] Ministerie van Infrastructuur en Milieu, „Aanpassen met ambitie: nationale klimaatadaptatiestrategie 2016 (NAS),” Den Haag, 2016.
- [5] Planbureau voor de Leefomgeving (PBL), „Hoe wordt Nederland klimaatbestendig?,” 2026.
- [6] TNO, „Klimaatrisico's voor de gebouwde omgeving (TNO 2026 R10004),” 2026.
- [7] Planbureau voor de Leefomgeving (PBL), „Nationale klimaatrisicoanalyse 2022-2026, Uitwerking analysemethodiek,” 23 maart 2023.
- [8] KNMI, „KNMI'23 klimaatscenario's voor Nederland,” 9 oktober 2023.
- [9] K. Fritzsche, S. Schneiderbauer, P. Bubeck, K. S. M. Buth, M. Zebisch en W. Kahlenborn, „The Vulnerability Sourcebook: Concept and guidelines for standardised vulnerability assessments,” German Agency for International Cooperation GmbH, Obrigheim, Germany, 2014.
- [10] K. Fritzsche, S. Schneiderbauer, P. Bubeck, S. Kienberger, M. Buth, M. Zebisch en W. Kahlenborn, „Indicator and data factsheet. Annex to The Vulnerability Sourcebook: Concept and guidelines for standardised vulnerability assessments,” German Agency for International Cooperation GmbH (GIZ), Obrigheim, Germany, 2014.
- [11] Planbureau voor de Leefomgeving (PBL), „Toekomstverkenning WLO: Vier scenario's voor Nederland in 2040, 2050 en 2060,” Den Haag, 2025.
- [12] Planbureau voor de Leefomgeving (PBL), [Online]. Available: Welvaart en Leefomgeving (WLO)-scenario's .
- [13] Deltares, „Deltascenario's 2024 Zicht op water in Nederland,” Delft, April 2024.
- [14] Planbureau voor de Leefomgeving (PBL), „Landbouw- en natuurverkenning - Op zoek naar een nieuwe balans tussen landbouw en natuur in 2050,” 29 oktober 2025.
- [15] International Organization for Standardization (ISO), „ISO 14091:2021 Adaptation to climate change — Guidelines on vulnerability, impacts and risk assessment,” 2021.
- [16] Intergovernmental Panel on Climate Change (IPCC) , „AR5 Climate Change 2014: Impacts, Adaptation, and Vulnerability. Contribution of working group II to the fifth assessment report,” 2014.
- [17] UK Department for Environment, Food & Rural Affairs, „UK Climate Change Risk Assessment 2022,” 2022.

- [18] Europese Commissie, „Digital Economy and Society Index (DESI) 2022 - Thematic chapters,” <https://digital-strategy.ec.europa.eu/en/policies/desi>, 2022.
- [19] Ministerie van Economische Zaken en Klimaat (MinEZK), „De staat van de digitale infrastructuur - De ruggengraat van onze digitale economie,” <https://open.overheid.nl/documenten/9c5f2d91-fafc-405e-b330-96d6211677bc/file>, 2024.
- [20] Deltares, „Kennisoeverzicht wateroverlast in relatie tot vitale en kwetsbare functies,” 2024.
- [21] Ericsson, „Ericsson Mobility Visualizer,” November 2025. [Online]. Available: <https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=1&ft=2&r=1&t=1,2,3,4,5,6,7,26&s=4&u=1&y=2025,2031&c=3>.
- [22] Interdigital, „Environmentally Sustainable 5G Deployment,” November 2020. [Online]. Available: https://www.interdigital.com/white_papers/environmentally-sustainable-5g-deployment.
- [23] Rijksoverheid, „Communicatiesysteem voor hulpdiensten C2000,” n.d.. [Online]. Available: <https://www.rijksoverheid.nl/onderwerpen/communicatie-hulpdiensten-c2000/c2000>.
- [24] Autoriteit Consument en Markt (ACM), „Marktbeschouwing telecommarkt 2024 (ACM/UIT/629572),” 2024.
- [25] Ministerie van Economische Zaken en Klimaat (MinEZK), „Actieplan duurzame digitalisering - De Digitale Sector Verduurzamen & Digitalisering Inzetten voor Verduurzaming,” Juni 2024.
- [26] NCTV, „CER en NIS2 richtlijnen,” [Online]. Available: <https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen>.
- [27] Minister van Justitie en Veiligheid, „Wetsvoorstel Wet weerbaarheid kritieke entiteiten,” [Online]. Available: <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36765>.
- [28] Minister van Justitie en Veiligheid, „Wetsvoorstel Cyberbeveiligingswet,” [Online]. Available: <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36764>.
- [29] Autoriteit Consument en Markt (ACM), „Telecommonitor eerste kwartaal 2025,” [Online]. Available: <https://www.acm.nl/nl/publicaties/acm-telecommonitor-eerste-kwartaal-2025>.
- [30] Stichting Climate Adaptation Services (CAS), „Klimaat-effectatlas,” [Online]. Available: <https://www.klimaat-effectatlas.nl/nl/>. [Geopend 10 December 2025].
- [31] B. Kolen, B. Strijker, D. Honingh, D. Lugt, M. Hoogvliet, N. Dolman, H. Nomden, R. Swinkels, R. Hulsman, S. v. d. Tillaart en J. Kind, „Methodiek voor uitwerken bovenregionale extreme neerslagsscenario's als input voor stresstesten, ruimtelijke ordening, crisisbeheersing en risico analyse,” NKWK, 2022.
- [32] D. Honingh, B. Kolen, B. Strijker, D. Lugt, J. Caspers, J. Kind, H. Nomden, J. d. Niet, S. Suijkens, S. v. d. Tillaart, M. v. Kouwen en C. Damen, „Methodiek voor een kwantitatieve risicodialoog en het opstellen van een bibliotheek met kritieke uitvalwaarden inclusief voorbeelden van beschermingsmogelijkheden van vitale infra,” NKWK, 2024.

- [33] E. Luijff en S. Oort, „Klimaatadaptatie en de sector Informatie- en Communicatie Technologie (ICT),” TNO, 2014.
- [34] P. Vermeulen, S. Grove, K. Verhoeven, P. Kokke en L. Beukers, „State of the Dutch Data Centers 2024,” Dutch Data Center Association, 2024.
- [35] S. Grove, P. Kokke, L. Beukers, M. Boeren en E. Lamberts, „Water usage in data centers,” Dutch Data Center Association, 2024.
- [36] SEO, „Nederlandse Innovatie Monitor 2025 Het innovatielandschap in een kwetsbare omgeving,” November 2025.
- [37] CBS, „Watergebruik binnen de Nederlandse economie; Milieurekeningen,” 12 November 2025. [Online]. Available: <https://opendata.cbs.nl/#/CBS/nl/dataset/82883NED/table>.
- [38] Uptime Institute, „Annual outage analysis 2025 (UII Keynote Report 173 • May 2025),” May 2025.
- [39] TCFD, „Task Force on Climate-related Financial Disclosures,” [Online]. Available: <https://www.fsb-tcfd.org/>.
- [40] IFRS, „ISSB and TCFD,” [Online]. Available: <https://www.ifrs.org/sustainability/tcfd/>.
- [41] D. Beijlaarts, „Kamerbrief Datacenters in de Nederlandse digitale economie,” 21 November 2024. [Online]. Available: <https://www.rijksoverheid.nl/documenten/kamerstukken/2024/11/21/kamerbrief-datacenters-in-de-nederlandse-digitale-economie>. [Geopend 2025].
- [42] Dutch Data Center Association, „State of the Dutch Data Centers 2025: From boom to bottlenecks,” 2025.
- [43] Directoraat-generaal Economie en Digitalisering, „Kamerbrief Datacenters in de Nederlandse digitale economie,” 16 Oktober 2024. [Online]. Available: <https://open.overheid.nl/documenten/6ef40415-8207-43cc-ba88-cae404bf1dac/file>. [Geopend 2025].
- [44] NCTV, „Wet weerbaarheid kritieke entiteiten,” [Online]. Available: <https://www.nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten>. [Geopend 2025].
- [45] Rijksoverheid, „Antennebureau,” [Online]. Available: <https://www.antennebureau.nl/plaatsing-antennes/aantal-antenne-installaties-voor-mobiele-communicatie>. [Geopend 6 januari 2026].
- [46] Cellnex Telecom, „Environment and climate change report,” https://www.cellnex.com/doc/ECC_Report_2023_English.pdf, 2023.
- [47] Koninklijke KPN N.V., „KPN integrated annual report 2023,” 2023.
- [48] Cellnex Telecom, „Integrated annual report 2024,” 2024. [Online]. Available: https://informeanualintegrado.cellnex.com/files/2024/Informe_Anuual_Integrado_2024_EN.pdf. [Geopend 2025].
- [49] S. O'Mahony, „Over one million users still without mobile coverage or broadband after Storm Eowyn,” Irish Independent, 26 Januari 2025. [Online]. Available: <https://www.independent.ie/irish-news/over-one-million-users-still-without-mobile-coverage-or-broadband-after-storm-eowyn/a2056651609.html>.
- [50] Stichting Dutch Data Center Association (DDCA), „State of the Dutch Data Centers 2024,” 2024.

- [51] Informatiepunt Leefomgeving, „Verdringingsreeks,” [Online]. Available: <https://iplo.nl/thema/water/beheer-watersysteem/verdringingsreeks/>. [Geopend 2025].
- [52] H. Oerlemans, „Datacenters slurpen drinkwater: Feit of Fictie?,” Koninklijke Nederlands Watersnetwerk (KNW), 2021.
- [53] Overheid.nl, „Regeling besluit kwaliteit leefomgeving,” 1 July 2024. [Online]. Available: <https://wetten.overheid.nl/BWBR0041313/2024-07-01>.
- [54] Google, „Google start met de bouw van een nieuw datacenter in Winschoten,” The Keyword (Google Blog), 14 December 2023. [Online]. Available: <https://blog.google/intl/nl-nl/google-nieuws/over-google/google-start-met-de-bouw-van-een-nieuw-datacenter-in-winschoten/>.
- [55] Businesswire, „ECL introduces world's first fully-green, hydrogen-powered, off-grid data center,” 24 January 2023. [Online]. Available: <https://www.businesswire.com/news/home/20230124005492/en/ECL-Introduces-Worlds-First-Fully-Green-Hydrogen-Powered-Off-Grid-Data-Center-as-a-Service-with-99.9999-Percent-Uptime-at-Significantly-Lower-Cost-Than-Traditional-Colocation-Data-Centers>.
- [56] Centraal Bureau voor de Statistiek (CBS), „Watergebruik binnen de Nederlandse economie; Milieurekeningen,” 2021. [Online]. Available: <https://www.cbs.nl/nl-nl/cijfers/detail/82883NED>. [Geopend 2025].
- [57] Dutch Data Center Association & Pathema, „Water usage in data centers,” 2024.
- [58] I. Van Zaanen, J. Van der Woude, R. Lodder en J. Appelman, „Eindrapport pilot waterprofielen industrie,” 2021.
- [59] Google, „Datacenterlocaties,” n.d.. [Online]. Available: <https://datacenters.google/intl/nl/locations/>.
- [60] Microsoft, „Explore the Microsoft datacenter regions,” n.d.. [Online]. Available: <https://datacenters.microsoft.com/globe/explore/>.
- [61] Drinkwaterplatform, „Waar komt ons kraanwater vandaan?,” 17 November 2021. [Online]. Available: <https://www.drinkwaterplatform.nl/themas/watertransitie/winningen/>.
- [62] DataCenterDynamics, „Google's London data center outage during heatwave caused by simultaneous failure of multiple redundant cooling systems,” 2 Augustus 2022. [Online]. Available: <https://www.datacenterdynamics.com/en/news/googles-london-data-center-outage-during-heatwave-caused-by-simultaneous-failure-of-multiple-redundant-cooling-systems/>.
- [63] Google Cloud, „Multiple Cloud products experiencing elevated error rates, latencies or service unavailability in europe-west2,” 19 Juli 2022. [Online]. Available: <https://status.cloud.google.com/incidents/fmEL9i2fArADKawkZAa2>.
- [64] Dutch Data Center Association, „Datacentergids 2021,” 2021. [Online]. Available: <https://www.dutchdatacenters.nl/publicaties/datacenter-gids-2021/>.
- [65] Sikkom, „Nieuwe studie wijst uit: Groningen staat in 2050 regelmatig onder water,” 18 Januari 2021. [Online]. Available: <https://sikkom.nl/actueel/Nieuwe-studie-wijst-uit-Groningen-staat-in-2050-regelmatig-onder-water-28183954.html>.
- [66] Climate Central, „Coastal Risk Screening Tool: Land projected to be below annual flood level in 2100,” n.d.. [Online]. Available:

- https://coastal.climatecentral.org/map/7/6.8982/53.5889/?theme=sea_level_rise&map_type=year&basemap=roadmap&contiguous=true&elevation_model=best_available&forecast_year=2100&pathway=ssp3rcp70&percentile=p50&refresh=true&return_level=return_level_1&rl_mode.
- [67] Provincie Noord-Holland, „Datacenterstrategie Noord-Holland 2025-2027,” Februari 2025. [Online]. Available: https://www.noord-holland.nl/bestanden/pdf/Economie_Werk/Datacenterstrategie%20NH%202025-2027.pdf.
- [68] Computable.nl, „Equinix opent datatoren op Science Park,” 5 Juli 2017. [Online]. Available: <https://www.computable.nl/2017/07/05/equinix-opent-datatoren-op-science-park/>.
- [69] Equinix, „Design for Data Center Resiliency to Reduce Downtime Risk,” 8 Juni 2023. [Online]. Available: <https://blog.equinix.com/blog/2023/06/08/design-for-data-center-resiliency-to-reduce-downtime-risk/>.
- [70] Deltares, „Huidige watergerelateerde klimaatrisico's in Nederland,” Deltares, 2024.
- [71] Deltares, „Afvoerverdeling Rijntakken bij hoogwater,” 2024.
- [72] R. van Beek, „Wat is het risico op dijkdoorbraak bij droogte?,” Universiteit Utrecht, 23 Juli 2018. [Online]. Available: <https://www.uu.nl/nieuws/wat-is-het-risico-op-dijkdoorbraak-bij-droogte>.
- [73] REOS, „Ruimtelijke strategie datacenters: Routekaart 2030 voor de groei van datacenters in Nederland,” Maart 2019. [Online]. Available: <https://open.overheid.nl/documenten/ronl-ee990385-1965-44fa-9bf1-a99262e46890/pdf>.
- [74] Deloitte, „The economic impact of disruptions to Internet connectivity,” Oktober 2016. [Online]. Available: <https://globalnetworkinitiative.org/wp-content/uploads/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf>.
- [75] Forbes, „Unplanned downtime costs more than you think,” 22 Februari 2022. [Online]. Available: <https://www.forbes.com/councils/forbestechcouncil/2022/02/22/unplanned-downtime-costs-more-than-you-think/>.
- [76] ITIC, „Hourly Cost of Downtime Report Part 1,” 3 September 2024. [Online]. Available: <https://itic-corp.com/itic-2024-hourly-cost-of-downtime-report/>.
- [77] Cabling, „Report: ICT downtime costs business \$4 million per year,” 11 Februari 2015. [Online]. Available: <https://www.cablinginstall.com/data-center/article/16472303/report-ict-downtime-costs-businesses-4-million-per-year>.
- [78] HLN, „Massale stroomstoring heeft Spanje bijna 400 miljoen euro gekost,” 6 Mei 2025. [Online]. Available: <https://www.hln.be/buitenland/massale-stroomstoring-heeft-spanje-bijna-400-miljoen-euro-gekost~a263463e7/>.
- [79] Deltares, „Rode draden klimaatrisico's voor weerbare responsorganisaties,” 13 November 2024. [Online]. Available: <https://nipv.nl/wp-content/uploads/2024/12/20241113-Deltares-Rode-draden-klimaatrisicos-voor-weerbare-responsorganisaties.pdf>.
- [80] NIPV, „Lessen uit crises en mini-crisis: Klimaatverandering en extreem weer,” Boom bestuurskunde, Den Haag, 2023.

- [81] M. v. Eeten, A. Nieuwenhuijs, E. Luijff, M. Klaver en E. Curz, „The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports,” *Public Administration*, 89(2), pp. 381-400, 2011.
- [82] Ministerie Justitie en Veiligheid (MinJenV), „Landelijk Crisisplan Natuurbranden,” 14 Mei 2025. [Online]. Available: <https://www.nctv.nl/documenten/2025/05/14/landelijk-crisisplan-natuurbranden>.
- [83] Ministerie I&W, „Landelijk Crisisplan Hoogwater en Overstromingen,” 6 Mei 2021. [Online]. Available: <https://www.dcc-ienw.nl/documenten/2021/mei/6/landelijk-crisisplan-hoogwater-en-overstromingen>.
- [84] NCTV, „Landelijk Crisisplan Digitaal,” 23 December 2022. [Online]. Available: <https://www.nctv.nl/documenten/2022/12/23/landelijk-crisisplan-digitaal>.
- [85] Ministerie Economische Zaken en Klimaat (MinEZK), „Nationaal Crisisplan Elektriciteit 2021,” Februari 2022. [Online]. Available: <https://www.nctv.nl/documenten/2022/03/15/nationaal-crisisplan-elektriciteit-2021>.
- [86] TenneT, „Systeembescherming en -herstel,” n.d.. [Online]. Available: <https://www.tennet.eu/nl/de-elektriciteitsmarkt/nederlandse-markt/systeembescherming-en-herstel>.
- [87] TenneT, „Robuuste communicatie en applicaties,” 18 Mei 2022. [Online]. Available: <https://tennet-drupal.s3.eu-central-1.amazonaws.com/default/2023-12/Robuuste%20communicatie%20en%20applicaties%20V2%20update%202023.pdf>.
- [88] NEN, „NEN 7510: Informatiebeveiliging in de zorg,” n.d.. [Online]. Available: <https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg>.
- [89] ICT&Health, „Kuipers: deel zorgsector krijgt extra digitale verplichtingen,” 18 December 2023. [Online]. Available: <https://www.icthealth.nl/nieuws/kuipers-deel-zorgsector-krijgt-extra-digitale-verplichtingen/>.
- [90] D. Campbell, „London NHS trust cancels operations as IT system fails in heatwave,” *The Guardian*, 21 July 2022.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl