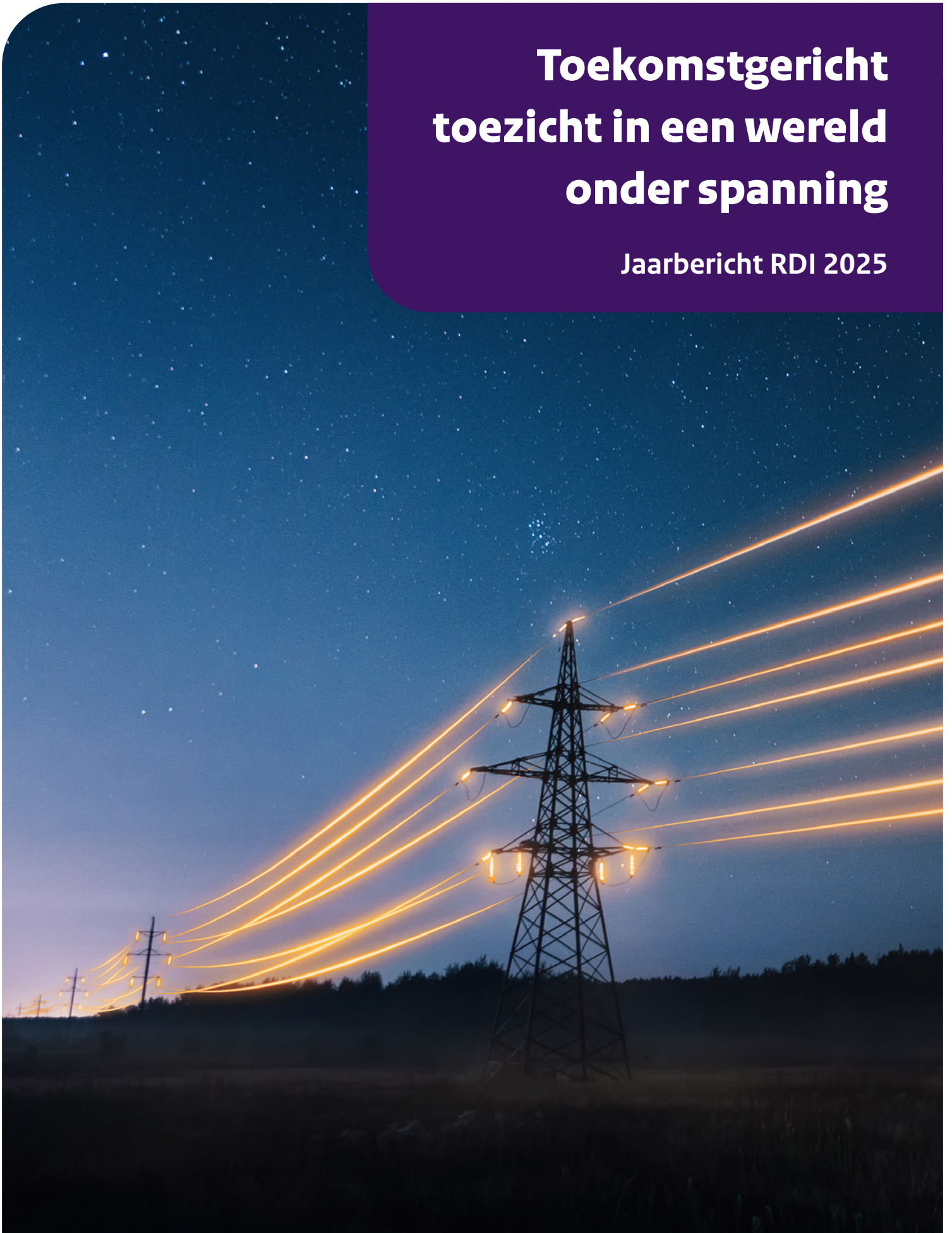




Toekomstgericht toezicht in een wereld onder spanning

Jaarbericht RDI 2025



Inhoud

VOORWOORD	4
Toezicht in een wereld onder spanning	
INLEIDING	6
De context van 2025	
Toezicht in samenhang	7
BESCHIKBAARHEID	9
Beschikbaarheid van digitale & analoge infrastructuren in een tijd van schaarste en geopolitieke druk	
Van onder de grond, tot in de ruimte	10
RDI waarborgt storingsvrije communicatie tijdens NAVO-top	11
Frequentiespectrum kent schaarste in sommige banden	11
Uitgifte/verdeling radio	11
Gezamenlijke Priority Control Area acties aan de grens	11
Ontwikkeling risico gestuurd en informatiegericht toezicht	12
Vorbereiding op de Cyberbeveiligingswet: het normenkader voor digitaal weerbare organisaties	12
Passende maatregelen digitale continuïteit en integriteit in Caribisch Nederland	12
Toezicht op kunstmatige intelligentie (AI)	13
Experimenteren en leren met de markt	13
BETROUWBAARHEID	15
Betrouwbaarheid van digitale systemen in een complexe en grensoverschrijdende omgeving	
Cybersecuritycertificering	16
Peer review (Europese review collega-toezichthouders op ons werk)	17
Future Network Services	17
AI-lab	17
Mobiele dekking	17
Samenwerkend toezicht voor uniformering in aanpak en kaders	18
Joint Activity projecten	18
Start voorbereiding nieuwe nationale markttoezicht strategie	18
Start toezicht op Europese Toegankelijkheidsrichtlijn	19
Convenant ontwikkeling met e-commerce platforms	19
Europese samenwerking bij gezamenlijke toezichtacties en internationaal overleg	19
Cyber Resilience Act (CRA)	19
VERTROUWEN	20
Vertrouwen in digitale infrastructuren als fundament voor een weerbare samenleving	
Asset Management (leveranciersketenmanagement)	21
Aanbieders van vast internet	22
Meldloket	22
Cyber spionage	22
Herziening 'New Legislative Framework' en ontwikkeling European Product Act	22
NIS2-zelfevaluatie en NIS2-Quickscan	22
Quantum	23
Vertrouwenstelsel Wettelijke Metrologie	23
Overleg met marktpartijen en voorlichting	23

Engiemeterwissel	24
Holland Solar	24
IACS-congres (NIS2)	24
AI-congres	24
INRICHTINGSBEPALLENDE WETGEVING	25
Wet- en regelgeving als fundament voor een zorgvuldige informatiehuishouding	
Informatie Voorziening (IV)	26
Informatiebeveiliging & Privacy	26
Algoritmeregister	27
Bijlage I: Kerncijfers	28

VOORWOORD

Toezicht in een wereld onder spanning



Toezicht in een wereld onder spanning

Geopolitieke spanningen spelen zich allang niet meer alleen af in de fysieke wereld. Zij raken direct de digitale infrastructuur waarop onze samenleving dagelijks vertrouwt. Netwerken, frequentieruimte en vitale verbindingen zijn strategisch geworden. Verstoring of uitval heeft onmiddellijke gevolgen voor maatschappelijke continuïteit, veiligheid én economische stabiliteit. Daarmee staat het publieke belang dat hiermee gemoeid is nadrukkelijk onder druk.

De Rijksinspectie Digitale Infrastructuur (RDI) opereert precies op dit snijvlak. Wij zien hoe digitale en fysieke infrastructuren samen het fundament vormen onder een weerbare samenleving en een goed functionerende economie. Beschikbaarheid, betrouwbaarheid en vertrouwen zijn daarbij geen vanzelfsprekendheden. Ze vragen om duidelijke kaders, zorgvuldige uitvoering en toezicht dat verder kijkt dan naleving alleen.

In 2025 heeft de RDI hieraan bijgedragen door toezicht te houden, vergunningen te verlenen, schaarse middelen zorgvuldig toe te delen en wettelijke waarborgtaken uit te voeren. Nieuwe (Europese) wetgeving en aanvullende opdrachten hebben het toezichtveld verbreed en verdiept. Dit maakt het werk van de RDI complexer en vraagt om scherpere keuzes. Niet aantallen of omvang staan centraal, maar hoe wij effect voor het publiek belang realiseren: probleem- en risicogericht, vanuit een stelselbenadering, met effectieve, proportionele interventies, onafhankelijk en betrouwbaar, en met oog voor de samenhang tussen fysieke en digitale belangen.

Die context vraagt om blijvende ontwikkeling van onze organisatie. Om vakmanschap, specialistische kennis en het vermogen om nieuwe technologieën en marktdynamiek te begrijpen. Toezicht moet meebewegen met innovatie, zonder publieke belangen uit het oog te verliezen. Als reflectieve toezichthouder leren wij van de praktijk, duiden wij signalen en scherpen wij onze aanpak voortdurend aan.

Samenwerking is daarbij essentieel. Met andere toezichthouders, met publieke partners en met marktpartijen. Alleen in samenhang kunnen wij risico's tijdig herkennen en bijdragen aan een weerbare digitale infrastructuur.

Met het meerjarenplan RDI 2026–2030 en in het licht van de nieuwe kabinetskoers kijken wij vooruit. Digitale weerbaarheid, een sterke infrastructuur, digitale soevereiniteit en een slagvaardige overheid zijn daarbij richtinggevend.

Dit jaarbericht laat zien wat de RDI in 2025 heeft gedaan, maar vooral ook wat wij hebben waargenomen. Welke ontwikkelingen vragen aandacht? Waar staan publieke belangen onder druk? En wat betekent dat voor toezicht in de komende jaren?

Want betrouwbaar, toekomstgericht toezicht op infrastructuren is onmisbaar in een wereld onder spanning.

mr. Angeline van Dijk,
Inspecteur-generaal Rijksinspectie Digitale Infrastructuur



INLEIDING

De context van 2025

A magnifying glass with a dark handle is positioned in the lower right, focusing on the year '2025' which is displayed in a large, white, digital-style font. The background is a complex, glowing blue circuit board with numerous lines and nodes, creating a sense of depth and technology. The overall color palette is dominated by various shades of blue, from deep navy to bright cyan.

2025

De context van 2025

In 2025 werkte de RDI in een omgeving waarin digitale infrastructuren steeds centraler staan in het functioneren van de samenleving. Internationale en technologische ontwikkelingen werken direct door in netwerken, verbindingen en systemen die burgers, bedrijven en instellingen dagelijks gebruiken.

Deze ontwikkelingen vergroten de afhankelijkheden binnen en tussen infrastructuren. Digitale en fysieke netwerken raken nauwer met elkaar verweven. Dat maakt verstoringen complexer en vergroot de aandacht voor beschikbaarheid, continuïteit en samenhang.

Tegen deze achtergrond zijn publieke belangen rond veiligheid, betrouwbaarheid en beschikbaarheid geen vanzelfsprekendheden. Goed functionerende digitale infrastructuren zijn randvoorwaardelijk voor innovatie en economische activiteiten in alle sectoren. De kwaliteit van infrastructuren beïnvloedt daarmee ook het vestigingsklimaat en de weerbaarheid van de economie.

Niet aantallen of omvang staan centraal, maar hoe wij effect voor het publiek belang realiseren: probleem- en risicogericht, vanuit een stelselbenadering, met effectieve interventies, onafhankelijk en betrouwbaar.

Deze context vraagt om een manier van werken waarin toezicht en uitvoering worden aangevuld met het tijdig signaleren en duiden van risico's. Dat gebeurt steeds vaker over domeinen en organisaties heen en in samenhang met andere toezichthouders en publieke organisaties.

Tegen deze achtergrond werkt de RDI langs samenhangende lijnen aan haar maatschappelijke opgave, met beschikbaarheid, betrouwbaarheid en vertrouwen als uitgangspunten.

Toezicht in samenhang

De maatschappelijke opgave van de RDI is bijdragen aan een veilig verbonden Nederland. Dit vraagt om toezicht dat verder gaat dan afzonderlijke domeinen of sectoren.

Vraagstukken rond digitale infrastructuur raken steeds vaker meerdere netwerken en partijen tegelijk.

Ketenafhankelijkheden nemen toe en verantwoordelijkheden zijn verdeeld. Effectief toezicht vraagt daarom om samenhang: het verbinden van signalen, het gezamenlijk duiden van risico's en het afstemmen van interventies.

De RDI richt zich niet alleen op toezicht achteraf, maar ook op het vroeg herkennen van ontwikkelingen die publieke belangen kunnen raken. Door signalen uit toezicht, uitvoering en het werkveld te combineren, ontstaat een beter beeld van risico's en kwetsbaarheden.

Toezicht in samenhang betekent ook dat de RDI oog heeft voor technologische innovatie en marktdynamiek. Toezicht moet aansluiten bij nieuwe toepassingen en ontwikkelingen, zonder publieke belangen uit het oog te verliezen.

Deze inzet wordt gestuurd door drie kernvragen:



*Is de infrastructuur aangelegd,
verbonden en weerbaar?*

*Zijn de netwerken en diensten continu
bereikbaar, integer en veilig?*

*Werken de apparaten en instrumenten
goed en veilig?*

Beschikbaarheid

De RDI draagt bij aan de beschikbaarheid van digitale en fysieke infrastructuren door toezicht te houden op aanleg, instandhouding en technische werking. Dit gebeurt onder meer via het beheer van het frequentiespectrum, het toekennen van gebruiksrechten en toezicht op werkzaamheden in de ondergrond.

Betrouwbaarheid

Wij richten ons op de betrouwbaarheid en continuïteit van netwerken en diensten. Door toezicht, signalering en duiding draagt de RDI bij aan de veiligheid, integriteit en weerbaarheid van vitale en essentiële dienstverleners.

Vertrouwen

De RDI werkt aan vertrouwen in de digitale infrastructuur door te zorgen voor veilige en betrouwbare producten en diensten, duidelijke kaders te stellen en te handhaven en oog te hebben voor de context waarin digitale toepassingen worden gebruikt.

In de praktijk komen deze drie kernvragen steeds vaker samen. Dat vraagt om samenhang in toezicht, om afstemming binnen en tussen netwerken van publieke en private partijen en om voortdurende reflectie op de rol van de RDI.

In de volgende hoofdstukken van dit jaarbericht wordt langs deze lijnen inzicht gegeven in de resultaten en observaties van het werk van de RDI in 2025.

BESCHIKBAARHEID

Beschikbaarheid van digitale & analoge infrastructuren in een tijd van schaarste en geopolitieke druk



Beschikbaarheid van digitale & analoge infrastructuren in een tijd van schaarste en geopolitieke druk

De Nederlandse samenleving rekt dagelijks op goed functionerende digitale en fysieke infrastructuren. Van mobiele netwerken en vaste verbindingen tot satellietcommunicatie en toepassingen in de ondergrond: zij vormen de basis voor economische activiteit, publieke dienstverlening en maatschappelijke continuïteit. Beschikbaarheid lijkt vanzelfsprekend, maar is dat niet.

In 2025 stond de beschikbaarheid van infrastructuren nadrukkelijk onder druk. Geopolitieke spanningen, toenemende afhankelijkheden en een groeiende vraag naar capaciteit maken schaarste zichtbaarder. Verstoringen in één onderdeel van het systeem kunnen zich snel verspreiden naar andere netwerken en sectoren. Beschikbaarheid is daarmee niet alleen een technisch vraagstuk, maar ook een strategisch, economisch en maatschappelijk vraagstuk.

De RDI draagt bij aan het borgen van deze beschikbaarheid door schaarse middelen, zoals frequentieruimte, zorgvuldig te verdelen op nationaal niveau, gebruiksrechten op het spectrum toe te kennen en hierover internationaal af te stemmen. Daarnaast houdt de RDI toezicht op de aanleg, instandhouding en storingsvrije werking van analoge en digitale infrastructuren. Ook ziet zij erop toe dat producten, diensten en systemen die op de markt komen geen verstoring veroorzaken en dat organisaties hun digitale weerbaarheid op orde hebben. Verder draagt zij bij aan de weerbaarheid van kritieke infrastructuur en vertrouwensdiensten. De RDI signaleert tijdig risico's die de continuïteit kunnen raken. In dit hoofdstuk laten we zien hoe de RDI in 2025 bijdroeg aan het versterken van de beschikbaarheid, betrouwbaarheid en weerbaarheid van digitale infrastructuren en systemen.

Van onder de grond, tot in de ruimte

Onder de grond

In de ondergrond zien we erop toe dat graafwerkzaamheden zorgvuldig worden uitgevoerd en schade aan kabels en leidingen wordt voorkomen. Graafschades zijn vervelend voor gebruikers, bijvoorbeeld wanneer een glasvezel- of energiekabel wordt geraakt, en kunnen zelfs onveilig zijn als een gasleiding wordt beschadigd. Het aantal graafschades blijft te hoog. Daarom hebben we in 2025 het boetebeleid aangescherpt om veroorzakers strenger te beboeten. Omdat we niet bij elke graafbeweging aanwezig kunnen zijn, zetten we daarnaast preventief in op gedragsinterventies om graafschades te voorkomen. We verwachten dat dit goed gedrag bevordert en in 2026 leidt tot een dalende trend, zodat de ondergrondse infrastructuur beschikbaar blijft voor gebruikers.

Ruimte

Vanuit de ruimte borgen we onder meer de betrouwbaarheid van navigatiesystemen als onderdeel van satellietsignalen. Internationaal zijn we betrokken bij discussies ter voorbereiding op besluiten over Direct-to-Device (D2D) tijdens de WRC-27. Deze besluiten gaan over beleid en regels rond technologie waarbij satellieten rechtstreeks met gewone apparaten (zoals smartphones) communiceren, zonder dat er een traditionele zendmast nodig is. Als nationale overheid maken wij daarnaast afspraken over het gebruik van de ruimte door Nederlandse bedrijven, in onze rol als Notifying Administration. In 2025 verleenden we een 15-jarige concessie voor satellietinternet op Bonaire, Sint-Eustatius en Saba. Hiermee is het aanbod aan internetdiensten uitgebreid. Aan de concessie zijn technische voorwaarden verbonden en verplichtingen voor de beveiliging tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van het netwerk in gevaar kunnen brengen.

RDI waarborgt storingsvrije communicatie tijdens NAVO-top

De continuïteit en het storingsvrij functioneren van de digitale infrastructuur is essentieel voor de economie en voor de veiligheid tijdens grote evenementen. Tijdens de NAVO-top van juni 2025 was de RDI, samen met het Ministerie van Defensie en de veiligheidsdiensten, nauw betrokken om verstoringen te voorkomen. De organisatie zorgde ervoor dat alle frequenties tijdens de top volledig beschikbaar bleven, zodat draadloze communicatie probleemloos kon functioneren. Dit soort werkzaamheden voert de RDI ook uit bij andere grootschalige publiekevenementen. Zoals de Formule 1 in Zandvoort, waar het storingsvrij gebruik van alle draadloze communicatie centraal staat. Van de 1-op-1 communicatie tussen coureur en team tot live televisie-uitzendingen, het mobiele gebruik van bezoekers en de communicatie van hulpdiensten.

In de aanloop naar de NAVO-top heeft de RDI daarnaast storende zonnepaneelinstallaties in een straal van 1.500 meter rondom een tiental essentiële C2000-antennes tijdelijk laten uitschakelen. Randapparatuur van dergelijke installaties kan storingen veroorzaken op de communicatie tussen portofoons en het C2000-netwerk. C2000 is het communicatiesysteem van hulp- en veiligheidsdiensten. In overleg met betrokken partijen werden deze installaties daarom vóór, tijdens en kort na de top buiten werking gesteld. Zodat de verbindingen van de veiligheidsdiensten betrouwbaar en storingsvrij bleven.

Frequentiespectrum kent schaarste in sommige banden

In opdracht van het Ministerie van Economische Zaken¹, heeft de RDI in nauwe samenwerking met een diverse groep van publieke en private stakeholders, een onderzoek gedaan naar de mogelijkheid Dynamic Spectrum Management and Sharing (DSMS). Simpel gezegd een onderzoek naar de mogelijkheden om schaarse frequentiebanden te kunnen delen. Zodat de schaarse frequentiebanden beschikbaar komen voor meerdere partijen en dus meer deelnemers van de maatschappij gebruik kunnen maken van het frequentiespectrum. De resultaten bieden zinvolle inzichten voor beleidsontwikkeling en een solide basis voor toekomstig onderzoek en follow-up pilots door geïnteresseerde marktpartijen, gericht op praktische en innovatieve spectrum sharing scenario's.

Binnen vooraf vastgestelde voorwaarden is het voor bedrijven mogelijk om binnen bepaalde frequentiebanden te experimenteren. Zo is het mogelijk om (gecontroleerd) nieuwe toepassingen te onderzoeken die (nog) niet in de reguliere wet- en regelgeving zijn opgenomen. Als RDI werken we graag samen met partijen samen aan dergelijke experimenteervergunningen.

Uitgifte/verdeling radio

Binnen het omroeplandschap is in 2025 een belangrijke stap gezet voor de continuïteit van regionale radio via zowel FM als de moderne DAB+ standaard. Omdat er meer vraag was dan aanbod, is ervoor gekozen de beschikbare frequentieruimte via een veiling te verdelen. De veilingen brachten in totaal ruim 5,5 miljoen euro op.

Gezamenlijke Priority Control Area acties aan de grens

In het tweede kwartaal van 2025 nam de RDI deel aan de actie Priority Control Area (PCA) e-commerce'. Deze actie richtte zich op consumentenproducten van zeer grote online platformen en marktplaatsen en werd geïnitieerd door de Europese Commissie. Samen met de Douane en de NVWA werden, tijdens elf actiedagen op Schiphol, administratieve en technische controles uitgevoerd vooral op elektronica en speelgoed.

De resultaten laten zien dat een groot deel van de gecontroleerde producten onbetrouwbaar was. Dat bevestigt dat het huidige e-commercestelsel onvoldoende waarborgen biedt voor productveiligheid en betrouwbaarheid. De PCA leverde waardevolle inzichten op voor toezicht aan de grens, waaronder het belang van gerichte productselectie, betere afstemming van capaciteit en verdere optimalisatie van douanefilters. Deze inzichten worden gebruikt bij de verdere ontwikkeling van het toezicht, waarbij data en signalen van onder andere de Douane worden ingezet om risicovolle producten eerder te selecteren voor controle.

De samenwerking met de Douane en andere toezichthouders werd als positief ervaren en vormt een goede basis voor verdere intensivering van het gezamenlijk toezicht op e-commerce aan de grens. RDI ziet er daarbij op toe dat producten die op de interne markt worden geplaatst geen storing veroorzaken en voldoen aan de geldende normen.

¹ In het hele document wordt Ministerie van Economische Zaken gebruikt, waar het verwijst naar de toekomst (na 23 februari 2026) is dat natuurlijk Ministerie van Economische Zaken en Klimaat

Ontwikkeling risico gestuurd en informatiegericht toezicht

In de snel veranderende context waarin de RDI opereert, is het belangrijk dat toezicht zich richt op de grootste maatschappelijke risico's. Daarom ontwikkelt de RDI het toezicht verder richting risico-gestuurd en informatiegericht werken en scherpt zij de bestaande risicomodellen aan, te beginnen bij het toezicht op producten.

De bevindingen uit onder meer de PCA-actie op e-commerce (zie hierboven) laten zien dat via grote online platforms regelmatig producten op de Nederlandse markt komen die administratief of technisch niet voldoen aan de regels. De mate van niet-naleving is hoog. In zo'n geval ontbreekt bijvoorbeeld documentatie, een Nederlandse handleiding of een correcte CE-markering. Omdat het productstelsel in de basis een vertrouwensstelsel is, begint naleving bij een correcte administratie.

Naast administratieve tekortkomingen blijken ook technische eisen regelmatig niet te worden nageleefd, met mogelijke risico's zoals brandgevaar of verstoring van netwerken.

Om deze risico's beter te adresseren zet de RDI in op betere risicoselectie binnen het toezicht. Daarbij wordt onder meer gebruikgemaakt van data van de Douane om risicovolle producten eerder te identificeren.

De RDI ontwikkelt hiervoor een integraal risicoafwegingskader. Daarmee kan de organisatie trends en risico's beter signaleren en het toezicht gericht inzetten waar de maatschappelijke impact het grootst is. Gezien de complexiteit van e-commerce zullen verbeteringen niet op korte termijn zichtbaar zijn, maar deze aanpak legt wel de basis voor effectiever toezicht.

Voorbereiding op de Cyberbeveiligingswet: het normenkader voor digitaal weerbare organisaties

De RDI heeft in 2025 belangrijke stappen gezet om zich voor te bereiden op de inwerkingtreding van de Cyberbeveiligingswet (CBW). De CBW implementeert de Europese richtlijn 'Network and Information Security'(NIS2). Met deze nieuwe wet komen duizenden nieuwe organisaties onder het toezicht van de RDI te vallen. Dit heeft er onder andere toe geleid dat de RDI een normenkader heeft ontwikkeld dat als basis dient voor het toezicht op digitale weerbaarheid, zoals bedoeld in de CBW. Digitale weerbaarheid gaat daarbij over het vermogen van organisaties om cyberdreigingen te voorkomen, incidenten tijdig te detecteren en verstoringen van hun netwerk- en informatiesystemen te beperken. Dit normenkader zorgt ervoor dat partijen gelijk worden behandeld en normen uit verschillende wetten duidelijk en uniform worden uitgelegd. Dit vergroot de rechtszekerheid, verlaagt de administratieve lasten en draagt bij aan betere naleving.

Door deze eenduidige manier van werken is de organisatie in staat om op basis van data te bepalen waar de grootste risico's binnen het toezicht liggen. Het doel is een effectieve inzet van de capaciteit zeker gezien de aanzienlijke uitbreiding van het aantal organisaties dat onder het toezicht van de RDI komt te vallen.

Een belangrijk onderdeel van de voorbereiding op het CWB-toezicht is het realiseren van een eenduidige manier van werken in de toezichtaanpak. Voor organisaties die moeten voldoen aan de CBW is het van groot belang dat toezichthouders dezelfde maatstaven en werkwijze hanteren. Om dit te realiseren is onder coördinatie van de RDI het samenwerkingsverband STDW (Samenwerkende Toezichthouders Digitale Weerbaarheid) opgericht.

Passende maatregelen digitale continuïteit en integriteit in Caribisch Nederland

De NIS2 is niet van toepassing op Caribisch Nederland. Enerzijds is het, gelet op de kleinschaligheid en beperkte middelen en expertise, niet haalbaar om deze regels onverkort van toepassing te laten zijn. Anderzijds loopt Caribisch Nederland het risico dat de continuïteit en integriteit van de telecommunicatie-infrastructuur onvoldoende wordt gewaarborgd. Om die reden zijn de concessies voor de mobiele netwerken aangevuld met voorschriften voor het treffen van passende technische en organisatorische maatregelen. Hiermee worden netwerken beter beveiligd tegen acties die de beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit in gevaar brengen. De concessies voor de vaste netwerken worden begin 2026 op dezelfde manier aangepast. De RDI houdt hierop toezicht en gaat samen met de concessiehouders inventariseren hoe open normen, zoals het treffen van beveiligingsmaatregelen, passend kunnen worden ingevuld.

Toezicht op kunstmatige intelligentie (AI)

Ontwikkeling van het toezicht

De RDI houdt sinds 2021 toezicht op het gebruik van kunstmatige intelligentie (AI). Dit sluit aan bij de toezichttaken van de RDI op digitale infrastructuur, producten en diensten die gebruikmaken van geautomatiseerde systemen.

Eind 2024 brachten Autoriteit Persoonsgegevens (AP) en de RDI namens alle toezichthouders een eindadvies uit over de inrichting van het toezicht van de AI-verordening in Nederland. In 2025 is de samenwerking tussen de twee nationale coördinerende toezichthouders geconcretiseerd in het AI Coördinatie Centrum Daarbij zijn afspraken gemaakt over de aansturing en samenwerking tussen toezichthouders.

Samenwerking met bedrijven en overheid

In 2025 is ook gestart met een bredere samenwerking met het bedrijfsleven en de overheid rondom AI en toezicht. In december organiseerden de gezamenlijke toezichthouders een congres waar zij in gesprek gingen met organisaties die onder de AI-verordening vallen. Tijdens dit congres werden de eindresultaten gepresenteerd van een gezamenlijk project van de RDI, de Europese Commissie en UNESCO over training voor toezicht op AI-systemen. Deze trainingen helpen toezichthouders AI-systemen integraal te beoordelen: niet alleen het product zelf, maar ook de context waarin het wordt gebruikt en regelgeving die daarop van toepassing is. UNESCO heeft ongeveer 700 toezichthouders uit meer dan 15 EU-lidstaten getraind. Hiervoor zijn onder meer casestudies, lesmateriaal en interactieve spellen ontwikkeld en is er online en offline documentatie beschikbaar.

Nationale regelgeving

Een belangrijke basis voor het toezicht vormt de Uitvoeringswet A-verordening, die wordt opgesteld door de Ministerie van Economische Zaken. De RDI levert een actieve bijdrage met adviezen over de uitvoerbaarheid en effectiviteit van het toezicht. Ook levert de RDI, rechtstreeks of via het ministerie, input aan de Europese Unie voor verdere uitwerking van het toezichtkader.

Europese samenwerking

Europese samenwerking is essentieel om dat AI-producten en bijbehorende risico's zich niet beperken tot de landsgrenzen. Onder leiding van de RDI kwamen in 2025 toezichthouders uit ongeveer 40 andere lidstaten zes keer bijeen om van elkaar te leren en toezichtspraktijken op elkaar af te stemmen. Zodat een vergelijkbaar AI-systeem in verschillende lidstaten op dezelfde manier wordt beoordeeld.

Mondiale samenwerking

Voor effectief toezicht op AI is ook samenwerking buiten de Europese Unie nodig. Veel AI-producten worden ontwikkeld buiten de EU of maken gebruik van internationale toeleveringsketens. Daarom lanceerden UNESCO en de RDI in juni 2025, tijdens het 3rd UNESCO 'Global Forum on the Ethics of Artificial Intelligence', het initiatief voor een mondiale samenwerking: 'Global Network of AI Supervisors'. In dit mondiale netwerk werken toezichthouders uit de verschillende werelddelen samen en het netwerk groeit snel.

Experimenteren en leren met de markt

In 2024 zijn de toezichthouders onder leiding van de AP en de RDI gestart met een pilot voor de **regulatory sandboxes** zoals opgenomen in de AI-verordening. De pilot is in 2025 geëvalueerd en zal naar verwachting in de loop van 2026 definitief van start gaan. In 2025 zijn voorbereidingen getroffen en is een vormvoorstel opgesteld voor de Nederlandse invulling van de regulatory sandboxes.

Een regulatory sandbox is een omgeving waarin bedrijven en toezichthouders met elkaar in gesprek gaan. In die gesprekken proberen ze samen duidelijkheid te krijgen over regels die nog niet helemaal helder zijn, vaak omdat het om nieuwe en innovatieve ontwikkelingen gaat.

Door deze samenwerking krijgen toezichthouders een beter beeld van wat er in de markt speelt. Tegelijkertijd worden de inzichten die ze opdoen gedeeld met andere partijen, zodat iedereen beter begrijpt hoe de regels moeten worden toegepast en innovatie gestimuleerd kan worden.

[Dit heeft geleid tot de oplevering van een concreet vormvoorstel voor de Nederlandse "regulatory sandbox" onder de AI-verordening.](#) Het eindrapport werd aangeboden aan de betrokken departementen en het vormvoorstel is gepubliceerd.

Sindsdien vormt het een inhoudelijke basis voor beleidsbeïnvloeding op Europees niveau. Op basis van de bevindingen leverden wij gerichte input voor de Europese Implementing Act, de nationale uitvoeringswet en de afstemming binnen de Europese werkgroep van de competent authorities on AI, met als doel de sandbox praktisch uitvoerbaar te maken en innovatie mogelijk te maken binnen duidelijke waarborgen voor veiligheid en publieke waarden.



BETROUWBAARHEID

**Betrouwbaarheid van
digitale systemen
in een complexe en
grensoverschrijdende
omgeving**

Betrouwbaarheid van digitale systemen in een complexe en grensoverschrijdende omgeving

Digitale infrastructuren functioneren in steeds complexere netwerken van producten, diensten en organisaties. Voor burgers en bedrijven lijkt de goede werking van deze systemen vaak vanzelfsprekend, maar achter die werking schuilt een uitgebreid stelsel van regels, certificering, standaardisatie en toezicht.

Een betrouwbare digitale infrastructuur begint bij duidelijke kaders en goed georganiseerd toezicht op publieke belangen. De RDI speelt daarin een rol als rijksinspectie, onder meer door het ontwikkelen en toepassen van certificeringsschema's onder de Cybersecurity Act (CSA), door toezicht te houden op de toegankelijkheid van digitale producten voor mensen met een beperking en door bij te dragen aan standaarden voor nieuwe Europese regelgeving zoals de Cyber Resilience Act (CRA).

Omdat veel digitale producten en diensten worden ontwikkeld en verhandeld in een Europese en mondiale markt, is internationale samenwerking essentieel. Dat vraagt om gezamenlijke kaders, afstemming tussen toezichhouders en een uniforme uitvoeringspraktijk binnen de Europese interne markt. De RDI neemt daarom actief deel aan Europese samenwerkingsverbanden en internationale standaardisatieprocessen.

Daarnaast draagt de RDI nationaal bij aan de betrouwbaarheid van digitale infrastructuren door vroegtijdig risico's te signaleren, vraagstukken te agenderen en samen met partners te werken aan oplossingen.

In dit hoofdstuk laten we zien hoe deze inzet in 2025 heeft bijgedragen aan het versterken van de betrouwbaarheid van digitale infrastructuren en digitale producten.

Cybersecuritycertificering

In 2025 heeft de RDI aanzienlijke stappen gezet richting een sterker en effectiever certificeringssysteem in Europa. Daarbij ligt de focus op de toegevoegde waarde van certificering binnen verschillende regelgevingen en de bijdrage aan het niveau van cyberveiligheid in Nederland en Europa. De RDI is enthousiast over deze ontwikkelingen en blijft investeren in kwaliteit en veiligheid binnen de digitale ruimte.

In de eerste helft van 2025 heeft de RDI aanzienlijke vooruitgang geboekt binnen het CSA-certificeringsprogramma met de toelating van twee certificerende instellingen en zeven testlaboratoria. Certificeringsschema's onder de Cybersecurity Act (CSA) bevatten cyberveiligheidseisen voor IT-producten en IT-diensten. Deze uitbreiding markeert een belangrijke stap in de groei van onze netwerksamenwerkingen en onze rol in de kwaliteitsbewaking van producten en diensten op Europees niveau. Het uiteindelijke doel is dat producten op de markt betrouwbaar zijn en voldoen aan hoge normen.

In de tweede helft van 2025 zijn de eerste certificeringstrajecten daadwerkelijk van start gegaan. Dit heeft geleid tot de goedkeuring van vier certificaten. Daarnaast zijn 30 onderzoeksplannen goedgekeurd die naar verwachting leiden tot nieuwe certificaten. Verwacht wordt dat tegen het einde van 2026 ongeveer 100 certificaten op het hoogste CSA-niveau zijn uitgereikt.

Het aantal certificaten groeit naar verwachting in 2027 verder, mede door het van kracht worden van verplichtingen voor marktpartijen onder de CRA, de NIS2-richtlijn, de AI-verordening en eIDAS2.

Daarnaast heeft de RDI, in nauwe samenwerking met de ministeries, schriftelijke input geleverd en gesprekken gevoerd met de Europese Commissie over de herziening van de CSA. De Europese Commissie publiceert het voorstel voor deze herziening in januari 2026.

Voor 2026 en de verdere toekomst staat de RDI voor de uitdaging om de capaciteit tijdig aan te passen aan de groei van nieuwe certificeringsschema's die in Europa van kracht zijn of in de komende jaren van kracht zullen worden. Deze tijdige aanpassing is cruciaal voor het uitvoeren van onze taken en het behoud van onze leidende rol in de cybercertificeringssector.

Peer review (Europese review collega-toezichthouders op ons werk)

Als reflectieve en transparante toezichthouder onderhoudt RDI continu nauw contact met collega-toezichthouders en externe stakeholders over de invulling van het toezicht. De RDI heeft in 2025 twee Europese collega-toezichthouders bereid gevonden om een peer review uit te voeren op het functioneren van de RDI voor de twee EU-richtlijnen op het terrein van meet- en weeginstrumenten. Onderdeel van de peer review was een bezoek aan de RDI in Amersfoort. De resultaten zijn vastgelegd in een openbaar rapport, dat is aangeboden aan samenwerkingsverbanden van Europese toezichthouders. De algemene conclusie van de peer review luidt dat de RDI een "goed georganiseerde, innovatieve en effectieve markttoezichtautoriteit" is. De RDI is uitgenodigd om in 2026 haar werkwijze toe te lichten aan de Europese collega's.

Future Network Services

De RDI en Nederland bereiden zich voor op de volgende generatie mobiele netwerken, namelijk 6G. De 6G-techniek beoogt voor business-to-business, machine-to-machine en in-factory draadloze connectiviteit te realiseren en zal rond 2030 beschikbaar komen. Met 6G smelten connectiviteit, IoT, AI en internet samen. Van onder de grond tot ver in de ruimte. Samen met onderzoekers, bedrijven en de overheid werkt de RDI samen om deze technologische doorbraak te realiseren. Future Network Services (FNS) is het door het Nationaal Groeifonds gefinancierd om bij te dragen aan betrouwbare en moderne telecommunicatie. Binnen FNS is onder andere het nationale 'testbed' van 6G fieldlabs opgezet. Het RDI-6G-fieldlab speelt daar een belangrijke rol in. Wij ondersteunen daarmee onder andere TNO in het gebruik van het testbed met onze technische expertise. Zo bereiden we Nederland nu al voor op de komst van 6G.

AI-lab

Sinds 2025 werkt het AI Lab (AI Safety & Security Lab) langs drie pilaren: Observatorium (vroeg signaleren en duiden van nieuwe AI-capaciteiten en risico's), Forensisch (ondersteuning van inspecties met bewijs dat standhoudt in het juridisch kader) en Dialoog (zichtbaar deelnemen aan het publieke debat en stakeholders verbinden). In 2025 brachten we de pilaren in de praktijk in een sterk geopolitiek veranderend speelveld en met nieuwe Europese verplichtingen: we bouwden kennis op en deelden die actief in het toezichtveld. Via onder andere ondersteuning bij de AI-verordening Sandboxes-pilot, samenwerkingsverbanden toezichthouders en daarbuiten met een AI Toezichtcongres en vaktechnische dagen. Daarnaast versterkte het AI-lab de Europese netwerksamenwerking via workshops binnen de Europese werkgroep van toezichthoudende autoriteiten op AI, ENISA en de Europese Commissie. Het AI Lab leverde inhoudelijke bijdragen aan en hielp met het organiseren van internationale panels en conferenties. Door daar zichtbaar en inhoudelijk aanwezig te zijn, laten we zien dat de RDI de techniek begrijpt en organisaties kan helpen met voorspelbaar en uitvoerbaar toezicht. Zo ontstaat sneller duidelijkheid en wordt innovatie gedreven door waarde en veiligheid, niet door het oprekken van grenzen.

Mobiele dekking

Om de betrouwbaarheid en kwaliteit van de dekking van het mobiele netwerk te garanderen voeren we controles uit in gemeenten. Met deze controles kijken we of mobiele netwerkoperators voldoen aan de dekking- en snelheidsverplichtingen en dus betrouwbaar zijn. In 2025 hebben we deze controles gedaan in 36 gemeenten, waaronder negen grensgemeenten. Uit de metingen blijkt dat er aan de gestelde eisen wordt voldaan. Dit bevestigt dat de mobiele dekking in Nederland tot de wereldtop behoort en de netwerken betrouwbaar zijn.

Samenwerkend toezicht voor uniformering in aanpak en kaders

In het overleg Samenwerkend Toezicht Digitale Weerbaarheid (STDW) werkt de RDI samen met alle toezichthouders² op de Cyberbeveiligingswet³ en de Wet weerbaarheid kritieke entiteiten aan samenwerkend toezicht. Binnen dit overleg maken toezichthouders gezamenlijk afspraken over het uitvoeren van hun toezichtstaak wanneer een entiteit te maken krijgt met meer dan één toezichthouder. Daarnaast vergelijken de deelnemende organisaties hun toezichtsbeleid en stemmen dit, waar mogelijk, op elkaar af. Hierin vervult de RDI een coördinerende rol.

Europese beleids- en netwerkvorming

De afgelopen jaren is de RDI vanuit digitale weerbaarheid actief en betrokken geweest bij meerdere Europese ‘work streams’ (inhoudelijke werkgroepen), waaronder die voor “Supervision” en “Energy”. Momenteel ligt de focus op de work streams “Digital infrastructure & Providers” en “Incident Reporting”. Door deel te nemen aan deze work streams bouwen en onderhouden we ons netwerk in Europa met Europese toezichthouders. Samen met andere toezichthouders zit de RDI hierdoor aan de voorkant van het beleidsproces waardoor wij actief kunnen bijdragen aan efficiënte en effectieve wetgeving. Dat helpt bijvoorbeeld in het zo laag mogelijk houden van de toezichtlast voor de markt.

Europese harmonisering van toezicht

Deze internationale gremia zijn plekken waar de RDI samenwerkt met andere EU-toezichthouders die op dezelfde onderwerpen actief zijn. Hier kan de RDI het gesprek met hen aangaan over de implementatie van de NIS2 richtlijn. Dit bevordert verdere harmonisering van toezicht op Europees niveau. Daarnaast ontstaat een betere mogelijkheid om gezamenlijk op te treden tegen partijen die in meerdere landen actief zijn.

Internationale samenwerking en kennisdeling

Het is ook nodig om met deze internationale collega-toezichthouder af te stemmen, omdat de NIS2-richtlijn samenwerking tussen staten verplicht. In internationaal overleg kunnen toezichthouders gezamenlijk verkennen hoe zij zo goed mogelijk kunnen voldoen aan die verplichte samenwerking, waarbij harmonisering opnieuw een belangrijke rol speelt. Daarnaast wordt er waardevolle kennis uitgewisseld, waarbij we soms inzichten delen over hoe wij ons werk doen, en soms juist kunnen leren van hoe andere toezichthouders de implementatie van de NIS2-richtlijn in hun land vormgeven. Dat draagt weer bij aan het vermogen om Nederland digitaal veilig verbonden en weerbaar te houden.

Joint Activity projecten

De RDI probeert continu zicht te houden op ontwikkelingen in het veld. In het metrologiedomein ontvingen de RDI en andere Europese toezichthouders een signaal van de Europese branchevereniging van leveranciers van weeginstrumenten (CECIP) dat online veel ongekeurde retail-weegschalen worden aangeboden. Hierdoor wordt het gelijke speelveld voor ondernemers verstoord. De RDI en collega-toezichthouders hebben daarom samen met de branchevereniging het de handschoen opgepakt om guidance op te stellen voor online aanbieders. Daarnaast is een gecoördineerde actie uitgevoerd waarbij een aantal retail-weegschalen is getest en zijn niet-nalevingen aangepakt bij de betrokken marktdeelnemers. Deze actie werd gefinancierd door de Europese Unie.

Guidance zijn niet-bindende uitingen van toezichthouders die bedoeld zijn om ondertoezichtstaanden te helpen maatschappelijk gewenst gedrag te laten zien. Guidance verduidelijkt regels, verwachtingen en goede praktijken, zonder dat er nieuwe verplichtingen ontstaan.

Start voorbereiding nieuwe nationale markttoezicht strategie

In 2025 is Nederland gestart met de voorbereiding van een nieuwe Nationale Markttoezicht Strategie voor Nederland. De RDI draagt bij aan die strategie. Deze strategie loopt van 2026-2030 en bepaalt in grote mate de prioriteiten voor Nederland in markttoezicht. Onderwerpen als: samenwerking aan de grens, kennisdeling, versterken van risico gebaseerd toezicht/ontwikkelen van voorspellende modellen, opleiden inspecteurs, digitalisering, versterken reflectieve functie van markttoezicht (signalen aan beleid) en andere overkoepelende thema’s horen hierin thuis. De strategie wordt samen met Nederlandse Voedsel- en Warenautoriteit, Inspectie Gezondheid en Jeugd, Inspectie Leefomgeving en Transport, Nederlandse Arbeidsinspectie, Douane en Ministerie van Economische Zaken ontwikkeld. De jaarplannen van RDI worden gekoppeld aan de prioriteiten uit de nationale strategie en tussentijds geëvalueerd.

2 [Cyberbeveiligingswet | Rijksinspectie Digitale Infrastructuur \(RDI\)](#)

3 [Wet weerbaarheid kritieke entiteiten | Rijksinspectie Digitale Infrastructuur \(RDI\)](#)

Start toezicht op Europese Toegankelijkheidsrichtlijn

Op 28 juni 2025 is de Europese Toegankelijkheidsrichtlijn (EAA) in werking getreden. Het doel van deze richtlijn is ervoor te zorgen dat specifieke producten en diensten toegankelijk zijn, zodat iedereen in onze maatschappij op gelijke voet kan meedoen. De RDI is aangewezen als toezichthouder.

Samenwerking met de andere Europese markttoezichthouders en ervaringsdeskundigen, zoals mensen met een beperking die dagelijks tegen toegankelijkheid aan lopen, is van wezenlijk belang om het doel van de richtlijn te behalen. We zijn onder andere gestart met kennisuitwisseling en deelname aan de werkgroep voor standaardisatie. We hebben webpagina's voor zowel de marktdeelnemers (fabrikanten, importeurs, distributeurs en dienstverleners) als de burgers ingericht met informatie over de richtlijn. Ook heeft de RDI samen met het ministerie van Volksgezondheid, Welzijn en Sport en de andere Nederlandse toezichthouders een meldloket voor consumenten gelanceerd. We hebben een beperkt aantal meldingen ontvangen, bijvoorbeeld over een touchscreen op een betaalterminal of een te hoog geplaatste betaalterminal. De RDI houdt risico gestuurd toezicht op producten en gaat in gesprek met de marktdeelnemers en de ervaringsdeskundigen om input voor het toezicht op te halen. Ons toezicht volgt het motto: zacht waar het kan, hard waar het moet. Zodat producten betrouwbaar en toegankelijk zijn voor eenieder die dat nodig heeft.

Convenant ontwikkeling met e-commerce platforms

De verkoop van producten via online platformen, e-commerce, is enorm populair. Ruim 40% van de Nederlanders geeft de voorkeur aan deze manier van aankopen en dit percentage zal naar verwachting groeien. De RDI toetst regelmatig of producten afkomstig van webshops voldoen aan de regelgeving. Vooral bij de grote, vaak buiten de Europese Unie gevestigde, online platformen ziet de RDI onvolkomenheden. Omdat het niet mogelijk is alle producten te controleren, wordt ingezet op het sluiten van een convenant. Daarin worden afspraken gemaakt over het snel verwijderen van producten waarvan duidelijk is dat ze niet voldoen aan de regelgeving. Verder wordt verkend op welke slimme manier gezamenlijk actief in de productdatabase gezocht kan worden naar producten die niet voldoen aan de regels. Een van Nederlands grootste webshops heeft inmiddels aangegeven zo'n convenant te willen afsluiten. Omdat de Europese regelgeving de online platformen in toenemende mate verplicht om aan toezicht mee te werken, wordt verwacht dat er meer convenanten gesloten zullen worden. Uiteindelijk moet alles ervoor zorgen dat de producten op de Nederlandse markt betrouwbaar zijn.

Europese samenwerking bij gezamenlijke toezichtacties en internationaal overleg

Omdat toezicht op productregelgeving onderdeel is van een Europese interne markt werkt de RDI nauw samen met andere Europese toezichthouders. De RDI doet mee aan gezamenlijke Europese campagnes. In 2025 deed de RDI mee aan twee onderzoeken: naar apparatuur voor zonnepaneelinstallaties en naar draadloze (5 GHz) apparatuur. In beide onderzoeken bleek dat sommige producten niet voldoen aan de veiligheidseisen. Deze onderzoeken vonden plaats in meerdere Europese landen. Bij zonnepaneelinstallaties kan apparatuur storing veroorzaken op vitaal frequentieverkeer. Nederland heeft hier relatief veel last van. Draadloze apparatuur in de 5-GHz band kan storing geven op weerradarinstallaties. Deze radarinstallaties zijn belangrijk voor de weersvoorspellingen voor defensie, burgers en bedrijven. Het KNMI vindt het daarom belangrijk dat de RDI hiertegen optreedt. Deze acties helpen bedrijven zich beter aan de regels te houden en vergroten het vertrouwen van de sector.

Cyber Resilience Act (CRA)

De RDI neemt actief deel aan de Europese werkgroepen om de beveiliging van digitale producten te verbeteren via toezicht op de Cyber Resilience Act (CRA). Daarnaast levert de RDI de projectleider van de belangrijkste Europese standaard voor de implementatie van de CRA. Alle fabrikanten, importeurs en distributeurs van producten met digitale elementen vallen onder de CRA. Om de partijen actief te informeren over de ontwikkelingen heeft de RDI, in samenwerking met het ministerie van EZ vijf webinars georganiseerd en acht keer gesproken op congressen en themabijeenkomsten. Dat heeft geleid tot waardevolle inzichten in de markt. Op het vlak van markttoelating organiseert de RDI informatiebijeenkomsten en voert zij gesprekken met geïnteresseerde partijen en andere lidstaten. De eerste aanmeldingen worden naar verwachting in de zomer van 2026 verricht. Daarmee zal Nederland waarschijnlijk het eerste land in Europa zijn met actief aangemelde instanties die producten kunnen certificeren. Dit moet ertoe leiden dat Nederland als een van de eerste landen betrouwbare en veilige producten op de markt heeft die voldoen aan de veiligheidsnormen, zodat Nederland veilig verbonden blijft.

VERTROUWEN

Vertrouwen in digitale infrastructuren als fundament voor een weerbare samenleving

Vertrouwen in digitale infrastructuren als fundament voor een weerbare samenleving

De samenleving digitaliseert in hoog tempo. Digitale infrastructuren en diensten spelen een steeds grotere rol in het dagelijks leven van burgers, bedrijven en overheden. Van communicatie en financiële transacties tot vitale processen in energie, zorg en mobiliteit: digitale systemen vormen steeds vaker de ruggengraat van onze samenleving. Dat maakt vertrouwen in deze systemen essentieel.

In 2025 stond dat vertrouwen onder druk. Geopolitieke spanningen, toenemende cyberdreigingen en afhankelijkheden in internationale leveranciersketens maken de kwetsbaarheid en weerbaarheid van digitale ecosystemen zichtbaar. Tegelijkertijd groeit het belang van toezicht op digitale weerbaarheid en op de manier waarop organisaties omgaan met risico's in hun infrastructuren en ketens.

De RDI draagt bij aan het versterken van dit vertrouwen door risico's inzichtelijk te maken, toezicht te houden op naleving van regelgeving en actief het gesprek te voeren met sectoren en stakeholders. In dit hoofdstuk laten we zien hoe deze inzet in 2025 vorm kreeg.

Asset Management (leveranciersketenmanagement)

De RDI deelt inzichten uit haar inspecties op het gebied van assetmanagement. Assetmanagement gaat over alle verschillende (operationele) eigendommen, hoe deze elkaar beïnvloeden en vervolgens het beheer daarvan. Zo kan bijvoorbeeld het uitvallen van een airco gevolgen hebben voor een serverruimte die van de koeling afhankelijk is. De RDI heeft bij 21 Aanbieders van Essentiële Diensten (AED's) in de energie- en digitale infrastructuursector een thema-inspectie naar assetmanagement uitgevoerd. Een betrouwbaar en actueel overzicht van alle kritieke assets vormt een onmisbare basis voor risicobeheersing en het garanderen van de continuïteit van essentiële dienstverlening. Dat uitgangspunt stond centraal in de inspecties: heeft de organisatie passende technische én organisatorische maatregelen getroffen voor goed asset management gedurende de hele levenscyclus van die eigendommen? Want 'als je niet weet wat je hebt, kun je het ook niet beschermen'. De resultaten zijn positief: er zijn geen overtredingen vastgesteld. Tegelijkertijd signaleerde de RDI wel enkele concrete verbetermogelijkheden. Met name in de OT-omgeving (Operationele Technologie) liggen kansen voor verdere versterking.

Verbeterpunten:

OT-assetregistratie verbeteren

Doordat de registratie van OT-assets (deels) handmatige plaatsvindt, is de registratie bij enkele AED's niet volledig of ontbreekt informatie over een eigendom. Automatisering van het registratieproces kan dit in sommige situaties verbeteren.

Afspraken met leveranciers aanscherpen

In (verouderde) OT-contracten ontbreken soms concrete security eisen en/of kritieke prestatie-indicatoren waarop gemonitord kan worden. Geadviseerd wordt om mogelijkheden te onderzoeken om contracten te vernieuwen of aan te vullen met een bijlage.

Update- en onderhoudsbeleid voor verouderde OT-systemen

Het actief en systematisch beheren, installeren en controleren van updates en onderhoud voor verouderde OT-systemen verdient aandacht. Bij enkele AED's ontbreekt dit.

Aanbieders van vast internet

De RDI houdt toezicht op aanbieders van vaste internetdiensten en -netwerken voor consumenten. Het gaat hierbij om diensten en netwerken via xDSL (digitale breedband verbindingen), kabel of glasvezel. Eerder heeft de RDI aangekondigd inspectie uit te voeren bij aanbieders van vaste internetdiensten. Met deze inspecties beoordeelt de RDI in hoeverre aanbieders voldoen aan de Telecommunicatiewet. Deze wet bevat onder meer regels voor veilige, betrouwbare en beschikbare telefoon- en internetnetwerken. De inspecties richten zich op drie hoofdonderwerpen uit de wet: de zorgplicht, de meldplicht en aftapbaarheid. De inspecties bestaan uit de volgende stappen: Er is een vragenlijst uitgezet bij een selectie van de aanbieders. Daarna volgen documentonderzoek en gesprekken op locatie. Hierdoor krijgt de RDI niet alleen inzicht in naleving van de Telecommunicatiewet, maar ook inzicht in de context waarin de aanbieders werken. Tot slot worden, wanneer dit nodig is, afspraken gemaakt om de naleving te verbeteren. De eerste resultaten zijn inmiddels gepubliceerd. De resultaten zijn positief maar tonen ook dat verdere verbetering nodig is om echt digitaal weerbaar te worden, te kunnen voldoen aan de huidige en toekomstige wetgeving, passend bij de huidige geopolitieke situatie. Zodat Nederland **veilig verbonden** is.

Meldloket

Telecomaanbieders hebben een meldplicht om beveiligingsincidenten met aanzienlijke gevolgen te melden bij het meldloket. Over 2025 heeft de RDI 27 meldingen via het meldloket ontvangen. Op basis hiervan onderneemt de RDI actie richting de betrokken partij. De analyses worden gedeeld met de RDI. Een belangrijk aspect hiervan is welke maatregelen de betrokken partij treft om herhaling van een dergelijk incident te voorkomen.

Cyber spionage

Eind 2024 werd de telecomsector geconfronteerd met een wereldwijde cyberspionagecampagne van de Chinese hackorganisatie Salt Typhoon. Deze ontwikkeling onderstreept het belang voor organisaties die onder toezicht van de RDI vallen om passende maatregelen te treffen ter versterking van de beveiliging van hun netwerken en diensten. Daarmee zorgen zij ervoor dat gevoelige informatie van Nederlandse burgers en organisaties zo goed mogelijk beschermd blijft. Als toezichthouder volgt de RDI deze en vergelijkbare ontwikkelingen in de telecomsector nauwlettend voor de opbouw van kennis.

Herziening ‘New Legislative Framework’ en ontwikkeling European Product Act

De Europese Commissie heeft, vanuit de “Better Regulation Agenda” en het strategisch rapport van Mario Draghi “The future of European competitiveness”, de ambitie om de Europese wetgeving aan te passen. Het doel is om het concurrentievermogen en de uitvoerbaarheid van regelgeving binnen de Europese markt te verbeteren. Het gaat niet om het verlagen van het beschermingsniveau, maar om het voorkomen van overlap tussen regelgeving en daarmee het verminderen van de administratieve lasten.

Ook wordt ingezet op verdere digitalisering en automatisering. De Europese Commissie werkt daarnaast aan de European Product Act. De RDI levert samen met andere toezichthouders een actieve bijdrage aan de uitwerking hiervan, richting het Ministerie van Economische Zaken en de Europese Commissie. Deze ontwikkeling vergroot het vertrouwen in de overheid doordat het stelsel van productregelgeving toekomstbestendig wordt gemaakt. Hierdoor kunnen burgers en bedrijven erop vertrouwen dat er betrouwbare producten op de markt komen en dat er een gelijk speelveld voor bedrijven bestaat.

NIS2-zelfevaluatie en NIS2-Quickscan

Samen met partners binnen de Rijksoverheid hebben we twee hulpmiddelen ontwikkeld voor organisaties om hen voor te bereiden op de komst van de Cyberbeveiligingswet (Cbw). Met behulp van de NIS2-Zelfevaluatie kunnen organisaties ontdekken of ze onder de NIS2 vallen of niet. Deze Europese richtlijn wordt omgezet in nationale wetgeving: de Cyberbeveiligingswet (Cbw). Het tweede hulpmiddel is de NIS2-Quickscan. Door 40 vragen in te vullen, krijgen organisaties inzicht in hoe de cyberbeveiliging van hun organisatie ervoor staat. In de scan staan ook andere sectoren die onder de Cbw vallen, dan de negen nieuwe sectoren waarop de RDI toezicht gaat houden.

De NIS-Zelfevaluatie is meer dan 205.000 keer geraadpleegd. Met 34.000 bruikbare datasets lijkt de NIS2 op 62% van de organisaties wel van toepassing en 33% niet van toepassing. De overige percentages vielen o.a. onder ‘nader te bepalen’.

De NIS2-Quickscan is 31.000 keer doorlopen. Hiervan hebben 6.100 organisaties de scan volledig ingevuld. Ze kregen daarbij handelingsperspectief: per thema ontvingen ze technische of organisatorische maatregelen die kunnen bijdragen aan de digitale weerbaarheid van hun organisatie.

Uit het algemene beeld van de NIS2-Quickscan van alle sectoren blijkt dat de volgende onderwerpen aandacht behoeven:

- Het trainen van alle leden van het bestuur (governance);
- De vermindering van de risico's van de toeleveranciersketen;
- De meldprocedures en rapportageverplichtingen.

Op [onze website](#) vinden organisaties veel informatie over alle bepalingen van de Cbw en hoe de RDI toezicht gaat houden.

Quantum

De kennis van de RDI wordt erkend door de buitenwereld. Wij nemen deel aan verschillende activiteiten en samenwerkingsvormen bij collega-overheden en sectorspecifieke kennisplatforms. Ook op Europees en internationaal niveau. RDI-medewerkers worden bijvoorbeeld gevraagd om op nationale en internationale conferentiepodia het perspectief van de toezichthouder te delen op de dreiging van de quantumcomputer. Dit onderwerp is zeer relevant aangezien quantumcomputers de manier waarop wij nu digitale informatie beveiligen door encryptie, fundamenteel veranderen. Met de komst van een volwaardige quantumcomputer bestaat er dus een groot maatschappelijk risico dat de huidige gebruikte encryptie kan worden doorbroken. Het is daarom cruciaal dat organisatie tijdig werken aan een quantum veilige digitale omgeving.

Niet alleen houdt de RDI de eigen kennispositie in stand door het blijven volgen van de ontwikkelingen op quantum-technologie, maar ook door het blijven informeren van partijen en het delen van kennis onderling. De RDI benadrukt de noodzaak voor passende en weloverwogen te nemen maatregelen, zoals quantumveilige encryptie, om deze kwetsbaarheid in de toekomst het hoofd te bieden. De RDI ziet dat haar bijdrage in de bewustwording en het draagvlak bij organisaties vergroot om stappen te zetten naar een quantumveilige omgeving. Dit blijkt bijvoorbeeld uit een toename van vragen over dit onderwerp van onder toezicht staande partijen. De RDI biedt hierbij richting en ondersteuning.

Vertrouwenstelsel Wettelijke Metrologie

We tanken brandstof en nemen elektriciteit af of leveren het juist terug. We rijden elektrisch of op waterstof en verwarmen of koelen ons huis met een warmte aansluiting. Voor het vertrouwen in een handelstransactie of belastingheffing is de juistheid van een hoeveelheid energie die je hebt afgenomen cruciaal voor je vertrouwen in de afspraak (transactie) met de leverancier. Daarom is een aantal soorten meetinstrumenten wettelijk geregeld.

Onder meer vanwege de energietransitie heeft de Europese Unie de belangrijkste Europese richtlijn voor meetinstrumenten (de Meetinstrumentenrichtlijn) aangepast en uitgebreid. De aanpassing was nodig omdat de richtlijn nog niet voorzorg in meetinstrumenten voor elektrische laadsystemen en andere meetinstrumenten van de energietransitie. Nederland is een van de lidstaten die hierop gewezen heeft. De aanpassing gebeurt in samenwerking met de lidstaten.

Het aanpassen van een richtlijn is een grote klus die veel afstemming, internationale samenwerking en expertise vereist. De RDI heeft hier veel expert-bijdragen geleverd. Veel van de Nederlandse bijdragen zijn overgenomen.

De aangepaste Meetinstrumenten-richtlijn is inmiddels door de Europese eerste onderhandelingsfase (triloofase), een onderdeel van de EU-besluitvorming. In 2026 zal de aangepaste Metrologierichtlijn door het Europees Parlement worden behandeld.

Overleg met marktpartijen en voorlichting

PPNIS2

Het publiek private samenwerkingsverband NIS2 (PPNIS2) is een samenwerking waar aan verschillende branche-organisaties en overheidspartijen deelnemen. Gezamenlijk doel is de informatiebehoefte van de markt en de communicatie vanuit de overheid over de CBW op elkaar af te stemmen en zo de markt voor te bereiden op de implementatie van de Cyberbeveiligingswet (CBW). Voor zowel de markt, als voor de RDI is dit een belangrijk verband om vragen over toezicht op de CBW en de informatiebehoefte van de markt af te stemmen. Dit maakt het mogelijk om vanuit RDI doelgericht guidance te bieden over thema's waar vanuit de markt de grootste behoefte ligt. Zoals de registratieplicht, bestuurlijke verantwoordelijkheid, en governance en risicomanagement.

Private 5G-netwerken

Voor de uitrol van de zogenoemde private 5G-netwerken gaat de RDI actief het gesprek aan met gebruikers en ander betrokken partijen. Met een perceelgebonden netwerk kan een organisatie een eigen draadloos netwerk gebruiken met een hoge capaciteit, snelheid en betrouwbaarheid. In 2025 sprak de RDI met diverse vergunninghouders in het havengebied van Rotterdam, de regio Eindhoven en andere delen van Nederland. De gesprekken geven de RDI meer inzicht in de voortgang van de uitrol van private 5G in Nederland en uitdaging waar partijen tegen aanlopen. Daarnaast helpen de gesprekken om het ecosysteem en de betrokken partijen beter in beeld te krijgen. Zo ontstaat een duidelijker beeld van de belangen en eisen van organisaties die overwegen over te stappen op een privaat 5G-netwerk dankzij het ontstane vertrouwen.

Energiemeterwissel

In 2025 hebben de voorbereidingen op de start van de energiemeterwissel plaatsgevonden. De Energiewet, waar de taak onder valt, ging in op 1 januari 2026 in. Vanaf januari 2026 krijgen mensen die nog een analoge meter hebben een brief van hun netbeheerder met een aanbieding voor een digitale meter of een slimme meter. Deze nieuwe meters kunnen de afname en teruglevering van eigen opgewekte elektriciteit apart registreren. Het verschil tussen een digitale en slimme meter is dat laatstgenoemde de meterstanden automatisch doorgeeft aan de energieleverancier.

De RDI is een maatschappelijk verantwoordelijke toezichthouder. Vanuit die gedachte hebben we het toezicht op de energiemeterwissel ingericht. We hebben in 2025 veel aandacht besteed aan de inrichting van het toezichtsproces aan de hand van gedragsinzichten. Zo is er een pre-test onder de doelgroep uitgevoerd om onze brieven te testen. Nadrukkelijk om de begrijpelijkheid van de brieven te toetsen. In samenwerking met het platform Steffie is een filmpje gemaakt die simpel uitlegt wat de energiemeterwissel betekent en wat er van de aangeschrevene wordt verwacht. Steffie is een platform gericht op laaggeletterden en mensen die de Nederlandse taal niet machtig zijn. De website wordt goed bezocht. We roepen in onze communicatie mensen op om hulp te vragen en contact te zoeken. We zien dat mensen ons weten te vinden en hun zorgen bij ons neerleggen, wat we positief vinden. Dat geeft ons de kans hen te helpen.

Holland Solar

Om informatie uit te wisselen over toenemende en complexere wetgeving en over ontwikkelingen in de markt, vindt er periodiek overleg plaats tussen de branchevereniging Holland Solar en de RDI. De ruim 250 leden van Holland Solar zijn actief in verschillende sectoren die relevant zijn voor de energietransitie. De focus voornamelijk op zonne-energie, maar ook energieopslag en energieopwekking zijn belangrijke onderwerpen. De uitwisseling van informatie biedt duidelijk meerwaarde voor beide organisaties: voor de sector zorgt dit voor meer duidelijkheid en snellere adoptie van nieuwe wetgeving, terwijl de RDI beter inzicht krijgt in het functioneren van het stelsel. De RDI heeft de ambitie om, in lijn met de samenwerking met Holland Solar, ook met ander brancheorganisatie vergelijkbare samenwerking te ontwikkelen.

IACS-congres (NIS2)

De RDI organiseerde op dinsdag 15 april 2025 een congres over 'Industrial Automation and Control Systems' (IACS) en Cybersecurity. Dit deed de RDI samen met het Nationaal Cyber Security Centrum (NCSC) en in samenwerking met de IACS-coalitie. De (verdergaande) digitalisering van fysieke processen door IACS brengt niet alleen voordelen met zich mee. Het laat ook de risico's van digitale dreigingen zien. Dit wordt onder andere onderschreven door de Nederlandse Cybersecuritystrategie (NLCS). Voor die dreigingen is aandacht voor in wetgeving, zoals de Wet Beveiliging Netwerken en Informatiesystemen (Wbni) en de opvolger daarvan: de Cyberbeveiligingswet. Tijdens het congres kwamen inspirerende sprekers aan het woord, brachten we initiatieven samen, was er ruimte om te netwerken en werden onderzoeken in dit vakgebied gedeeld.

AI-congres

Toezichthouders, bedrijven en experts ontmoetten elkaar op het AI-Toezichtcongres 2025 om de dialoog aan te gaan over verantwoorde én innovatieve inzet van AI. Het congres is georganiseerd door de RDI samen met de Autoriteit Persoonsgegevens. De bezoekers werden meegenomen in de inrichting van het toezicht, de inhoud van de AI-verordening en nationale en Europese samenwerkingen. In interactieve sessies ging men met elkaar in gesprek over innovatie, standaarden, regulatory sandboxes en nog veel meer onderwerpen rondom verantwoord AI-gebruik. Kerndoel was een start te maken met de samenwerking tussen toezichthouders, de markt en overheden die aan de AI-verordening moeten voldoen. De dialoog dient vertrouwen te geven in het AI-ecosysteem en hoe de toezichthouders te werk zullen gaan.



INRICHTINGSBEPALLENDE WETGEVING

Wet- en regelgeving als fundament voor een zorgvuldige informatiehuishouding

Wet- en regelgeving als fundament voor een zorgvuldige informatiehuishouding

De RDI streeft ernaar een reflectieve, betrouwbare en transparante toezichthouder te zijn en een publieke dienstverlening te leveren die aansluit bij de verwachtingen en behoeften van burgers en ondernemers. De inrichtingsbepalende wetgeving vormt de basis voor de richtlijnen en kaders die de RDI hanteert bij het inrichten van de informatiehuishouding. Deze kaders en richtlijnen zorgen voor samenhang tussen de visie op dienstverlening, het beleid en de uitvoering. Zij ondersteunen bovendien de sturing op kwaliteit en de continue verbetering van de dienstverlening aan de maatschappij.

In dit hoofdstuk laten we zien hoe deze wet- en regelgeving richting geeft aan de inrichting en verdere ontwikkeling van de informatiehuishouding van de RDI.

Informatie Voorziening (IV)

De groei van het aantal taken en de toenemende complexiteit van het werkveld vragen om een verdere versterking van onze informatievoorziening. De sterke groei van onder andere het aantal ondertoezichtgestelden maakt informatiegestuurd werken steeds belangrijker. Daarom werken we aan de doorontwikkeling van ons IV-landschap. In 2025 hebben we een analyse van de IV-organisatie uitgevoerd. Op basis daarvan is een actieplan voor verdere verbetering opgesteld. Met dit actieplan versterken we onder meer de beschikbare capaciteit, de ontwikkelmogelijkheden en de kwaliteit van onze processen. Daarnaast zijn we gestart met een verbeterde organisatiestructuur die het mogelijk maakt beter te sturen op standaardisatie en op effectieve oplossingen die binnen de hele organisatie toepasbaar zijn. Hiermee versterken we de basis voor een toekomstbestendige informatievoorziening en borgen we dat de RDI ook op lange termijn een effectieve toezichthouder blijft.

Informatiebeveiliging & Privacy

Vanuit haar toezichthoudende taken op het gebied van telecommunicatie- en IT-netwerken vervult de RDI een voorbeeldfunctie in het veilig omgaan met informatie. Daarom stellen wij hoge eisen aan de vertrouwelijkheid en integriteit van de gegevens die wij verwerken.

In het afgelopen jaar hebben we een TIBER-test laten uitvoeren om de weerbaarheid van onze digitale beveiliging te toetsen. Een TIBER-test (Threat Intelligence Based Ethical Red Teaming) is een realistische cyberoefening waarbij ethische hackers, op basis van actuele dreigingsinformatie, proberen in te breken in systemen om kwetsbaarheden in de digitale weerbaarheid bloot te leggen. De bevindingen zijn gebruikt om onze beveiligingsmaatregelen en dienstverlening verder te versterken.

Daarnaast zijn technische aanpassingen aan ons zaakstelsel doorgevoerd om te voldoen aan de vereisten van DigiD. Ook zijn beleid en richtlijnen binnen de organisatie aangepast om aan de vereisten van NIS2-wetgeving te voldoen. In 2025 heeft de RDI bovendien haar crisisparaatheid verder versterkt. Het Business Continuity Management plan voor de interne organisatie is herzien. Daarbij zijn de kritieke processen opnieuw vastgesteld en is een eerste cyberoefening uitgevoerd met het crisisteam en het vervangende crisisteam. Met deze verbeteringen verstreken wij onze weerbaarheid en zijn we beter voorbereid om Nederland veilig verbonden te houden, ook in tijden van verhoogde dreiging of incidenten.

Algoritmeregister

Om transparant te zijn over het gebruik van algoritmes en AI in onze dienstverlening heeft de RDI een volledige inventarisatie uitgevoerd van de algoritmes die binnen de organisatie worden gebruikt en ontwikkeld. Momenteel zijn binnen de RDI twaalf algoritmes in gebruik en zijn drieëntwintig algoritmes in ontwikkeling. Ook algoritmes waarvan de ontwikkeling tijdelijk is stilgelegd worden geregistreerd, wanneer verwacht wordt dat deze in een later stadium verder worden ontwikkeld.

Bij het bepalen of en op welke wijze algoritmes worden gepubliceerd, volgt de RDI de handreiking van het Algoritmeregister. De RDI richt zich op dit moment op de publicatie van algoritmes die daadwerkelijk binnen de organisatie worden toegepast.

In 2025 zijn twee impactvolle algoritmes opgenomen in het Algoritmeregister. In het eerste kwartaal van 2026 wil de RDI nog eens zeven algoritmes publiceren.

Bijlage I: Kerncijfers



Organisatie kerncijfers

	Realisatie 2021	Realisatie 2022	Realisatie 2023	Realisatie 2024	Realisatie 2025
Totaal aantal fte's	373,8	391,1	424,3	482,4	497,4
Kosten inhuur externen (x 1.000 euro)	8.352	8.286	10.391	10.028	11.966
Ziekteverzuim	3,0%	4,5%	4,3%	4,6%	4,6%
Percentage vrouwen	30%	32%	32%	32%	35%
Gemiddelde leeftijd	51,0	49,2	48,8	46,6	46,1

Financiële kerncijfers

	Realisatie 2021	Realisatie 2022	Realisatie 2023	Realisatie 2024	Realisatie 2025
Bedrijfsresultaat (x 1.000 euro)	-268	-586	1.219	3.846	3.597
Omzet (incl. Caribisch Nederland) (x 1.000 euro)	60.703	65.871	75.184	90.474	101.457
Personeelskosten per fte (x 1.000 euro)	100,3	103,6	114,6	116,8	123,8
Opleidingskosten als percentage van de personele kosten	1,74%	1,43%	1,66%	2,07%	1,48%
Huisvestingskosten per fte (x 1.000 euro)	7,2	9,4	7,8	8,3	8,3
Uurtarief (wijziging in reële termen)	1,59%	3,53%	0,00%	0,00%	-2,51%

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

📍 Emmasingel 1 Groningen

☎ 088 041 60 00

✉ info@rdi.nl

🌐 www.rdi.nl

April 2026



#wijzijnRDI