



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Verantwoord verweven?

*Veiligheid en beschikbaarheid van digitale
infrastructuur zijn geen vanzelfsprekendheid*

Meerjarenplan 2026-2030



Inhoudsopgave

De inspecteur-generaal aan het woord

Verhogen weerbaarheid is essentieel voor digitale veiligheid	4
---	----------

Hoe wij werken als RDI

Werken aan onze maatschappelijke opgaven als rijksinspectie	6
--	----------

Beschikbare technische infrastructuren	6
--	---

Security en weerbaarheid van netwerken en diensten	6
--	---

Veilige en betrouwbare producten	6
----------------------------------	---

Als organisatie klaar voor de opgaven van de toekomst	7
--	----------

Een integrale, brede blik op de goede werking van het stelsel	7
---	---

Een informatiegestuurd en risicogerichte benadering staat centraal in ons werk	7
--	---

Een eigenstandige positie en reflectieve rol in het stelsel	7
---	---

Vier kernactiviteiten	8
-----------------------	---

Belangrijkste strategische ontwikkelingen

Meerjarenperspectief op een hoogwaardige digitale infrastructuur	10
---	-----------

Gesignaleerde ontwikkelingen en maatschappelijke risico's	10
---	----

Waar wij in gezamenlijkheid op willen inzetten	11
--	----

De focus van de RDI voor 2026

Goede werking infrastructuur essentieel voor economie en samenleving	14
---	-----------

Maatschappelijke opgave, doelen en resultaten	14
---	----

Maatschappelijke risico's met impact op resultaten	14
--	----

Focuspunten	15
-------------	----

Samenleving vertrouwt op weerbare digitale infrastructuur	17
--	-----------

Maatschappelijke opgave, doelen en resultaten	17
---	----

Maatschappelijke risico's met impact op resultaten	18
--	----

Focuspunten	18
-------------	----

Producten nu en in de toekomst veilig en betrouwbaar	20
---	-----------

Maatschappelijke opgave, doelen en resultaten	20
---	----

Maatschappelijke risico's met impact op resultaten	21
--	----

Focuspunten	22
-------------	----

Samenwerken aan een weerbare infrastructuur voor Caribisch Nederland	23
---	-----------

Maatschappelijke opgave, doelen en resultaten	23
---	----

Maatschappelijke risico's met impact op resultaten	23
--	----

Focuspunten	24
-------------	----

De RDI als organisatie in beeld

Organisatiecijfers	26
---------------------------	-----------

Onze begroting voor 2026	26
--------------------------	----

RDI in Fte's	27
--------------	----

A pair of hands holds a white rectangular card against a solid blue background. The card features the text 'De inspecteur-generaal aan het woord' in a bold, blue, sans-serif font. The hands are positioned on the left and right sides of the card, with fingers visible at the edges. The background is a uniform, vibrant blue.

**De
inspecteur-
generaal
aan het
woord**



Verhogen weerbaarheid is essentieel voor digitale veiligheid

Digitalisering in onze maatschappij vindt plaats in een wereld die in hoog tempo verandert. Technologie opent ongekende mogelijkheden: nieuwe markten, andere manieren van werken en een vrijwel onuitputtelijke bron aan kennis via AI. Voor sectoren als gezondheidszorg en onderwijs of op het gebied van duurzaamheid biedt dit enorme kansen.

Tegelijkertijd brengen deze ontwikkelingen risico's met zich mee. Afhankelijkheid van digitale systemen en producten, en van leveranciers van diensten van landen buiten de EU maken ons kwetsbaar. Deze dreigingen kunnen zowel individuen als de samenleving als geheel raken. De vraag hoe verantwoord onze verwevenheid met digitalisering is, geeft mede richting aan ons werk. Ook als die buiten onze formele bevoegdheid ligt.

In de digitale infrastructuur participeren veel partijen. Verschillende technische systemen en onderdelen werken nauw samen in de keten en zijn onlosmakelijk met elkaar verweven. Dit maakt de digitale infrastructuur gelaagd en complex, waarbij de veiligheid van elke schakel de weerbaarheid van de gehele keten mede bepaalt. Geopolitieke spanningen, risico's van cloudopslag in het buitenland, veiligheidsrisico's van AI-systemen, kwetsbare met internet verbonden producten en internationale afhankelijkheden vergroten deze kwetsbaarheid. Versterking van digitale weerbaarheid is daarom een noodzaak.

Deze ontwikkelingen hebben een groeiende impact op ons werk en vragen van ons de nodige, extra inspanningen. In een tijd waarin hybride en militaire dreiging steeds dichterbij komen, zorgen wij ervoor dat Defensie ruimte krijgt om hier adequaat op in te spelen. Verder zien wij dat steeds meer organisaties belangrijk zijn voor onze (digitale) weerbaarheid, waardoor wij extra inzetten om ons inzicht in die partijen te vergroten. Daarnaast intensiveren wij ons toezicht op producten die Nederland binnen komen die niet voldoen aan de vereiste kwaliteitseisen ten behoeve van de veiligheid en weerbaarheid van Nederland.

Met focus, flexibiliteit en intensieve samenwerking met publieke en private partners in ons netwerk wil de Rijksinspectie Digitale Infrastructuur (RDI) voorzien in de noodzaak om onze digitale weerbaarheid te versterken. Daarbij waken wij onder meer over het frequentielandschap en verantwoorde AI-toepassingen. Wij bevorderen de cyberweerbaarheid van de maatschappij en houden toezicht op vitale sectoren, netwerken, informatiesystemen, de cyberveiligheid van producten en diensten – in lijn met (nieuwe) Europese regelgeving.

In recente wetgeving is steeds meer aandacht voor maatregelen die risico's als gevolg van de ontwikkelingen adresseren, maar het proces van wetgeving loopt tegelijkertijd achter op de ontwikkelingen. Wij zien daarom een grote opgave op ons afkomen, waarbij wetgeving en de aanwijzing voor de RDI als toezichthouder op deze nieuwe taken nog niet klaar is. Een deel van ons toezicht bevindt zich daardoor nog in een voorbereidende fase. Toch blijven wij vooruitlopend op regulering vanuit een brede blik al signaleren en agenderen.

Dit meerjarenplan biedt inzicht in de belangrijkste ontwikkelingen, en schetst risico's en focus van de RDI voor 2026 en daarna. Het vormt de leidraad voor onze gezamenlijke inspanningen om Nederland digitaal weerbaar en veilig verbonden te houden. Daarnaast geeft het richting aan ons toezicht, zodat wij blijvend bijdragen aan het verhogen van de weerbaarheid van de digitale infrastructuur.

mr. Angeline van Dijk
Inspecteur-generaal
Rijksinspectie Digitale Infrastructuur



Hoe wij werken als RDI





Werken aan onze maatschappelijke opgaven als rijksinspectie

Digitalisering is in toenemende mate verweven geraakt met bijna alle aspecten van ons dagelijks leven. Zij biedt grote kansen voor de maatschappij en economie. Tegelijkertijd groeit de maatschappelijke afhankelijkheid van digitalisering en nemen dreigingen en potentiële verstoringen toe. Daarom zorgt de RDI ervoor dat wij maatschappelijke vraagstukken rond de digitale infrastructuur tijdig detecteren, risico's signaleren en belangen beschermen. Onze maatschappelijke opgave is een veilig verbonden Nederland, zodat iedereen in Nederland kan vertrouwen op een digitale infrastructuur, die continu beschikbaar is en veilig gebruikt kan worden. Daarom richten wij ons op de volgende maatschappelijke vraagstukken:



*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?*

Vanuit deze maatschappelijke vraagstukken werken wij aan de volgende drie opgaven om de publieke belangen zo goed mogelijk te beschermen en Nederland veilig verbonden te houden.

Beschikbare technische infrastructuren

De Nederlandse samenleving rekent op een hoogwaardige analoge en digitale infrastructuur. De RDI bevordert en beschermt de beschikbaarheid van draadloze en draad gebonden netwerken, de dekking en capaciteit van die infrastructuur en een goede, storingsvrije werking hiervan. Dit doen wij onder andere door het frequentiespectrum in internationaal en nationaal verband te verdelen. De gebruiksrechten op dat spectrum toe te kennen en, waar dat vanuit onze toezichtstaak noodzakelijk blijkt, in te trekken. Ook zien wij erop toe dat graafwerkzaamheden in de ondergrond zorgvuldig worden uitgevoerd, om schade aan kabels en leidingen te voorkomen.

Security en weerbaarheid van netwerken en diensten

Wij zien toe op de continuïteit, integriteit, vertrouwelijkheid en authenticiteit van de digitale infrastructuur, zodat consumenten en ondernemers, die hun diensten via de digitale infrastructuur aanbieden, daar ongestoord en in vertrouwen gebruik van kunnen maken. Dit doen we onder andere door het borgen van een betrouwbaar stelsel van digitale producten, diensten en processen, zoals voor elektronische identificatie en authenticatie bij toegang tot de overheid. Wij bewaken en stimuleren de digitale weerbaarheid van vitale en essentiële dienstverleners in sectoren als telecom, internet en energie. Daarnaast informeren wij de maatschappij over het belang van de eigen digitale weerbaarheid ten aanzien van (rest)risico's.

Veilige en betrouwbare producten

Bovendien zetten wij ons in voor veilige en betrouwbare (digitale) producten die gebruikt worden binnen, of een onderdeel zijn van, de digitale infrastructuur. Nederland kan erop vertrouwen dat producten onder duidelijke randvoorwaarden en volgens geldende regelgeving in de handel zijn gebracht. En dat producten storingsvrij werken, elektrisch en elektromagnetisch veilig zijn, een correcte hoeveelheidsinformatie



bij handelstransacties weergeven, toegankelijk en cybeveilig zijn. Dit doen wij onder andere door te werken aan het stellen van kaders die veilige en betrouwbare producten waarborgen. De veiligheid en betrouwbaarheid van producten geldt niet alleen voor de fysieke componenten, maar in toenemende mate ook voor digitale componenten, zoals software, data, cloud toepassingen en andere digitale diensten. Daarnaast is ook de omgeving waarin deze digitale producten gebruikt worden steeds meer van belang, omdat commercieel verkrijgbare producten eenvoudig in vitale omgevingen gebruikt kunnen worden.

Als organisatie klaar voor de opgaven van de toekomst

Het belang van de digitale infrastructuur groeit en synchroon daaraan groeit de organisatie van de RDI mee; grotere complexiteit, meer regels om op toe te zien, nieuwe stakeholders en ondertoezichtgestelden. Om te bepalen hoe wij ons toezicht organiseren, heeft de RDI drie strategische organisatiedoelen geformuleerd.



Een integrale, brede blik op de goede werking van het stelsel



Een informatiegestuurde en risicogerichte benadering staat centraal in ons werk



Een eigenstandige positie en reflectieve rol in het stelsel

Een integrale, brede blik op de goede werking van het stelsel

Wij kennen het stelsel en de spelers, zodat wij de juiste positie kunnen innemen om effectief te beïnvloeden. Dat vraagt van ons dat wij de komende jaren investeren in de wijze waarop wij samen met netwerkpartners en ketenpartners een veilig verbonden Nederland realiseren. Wij blijven onderzoek doen om onze kennis te vergroten en delen deze resultaten met onze stakeholders.

Een informatiegestuurde en risicogerichte benadering staat centraal in ons werk

Wij hebben zicht op kansen en risico's in de digitale infrastructuur, zitten aan de 'voorkant' en zijn betrokken bij (internationale) beleidsvorming en regelgeving. Wij verkennen actief technologische en maatschappelijke ontwikkelingen en blijven inzetten op het verder ontwikkelen van onze informatiegestuurde en risicogerichte benadering vanuit onze integrale toezichtvisie. Hiermee investeren wij in het continu vernieuwen van ons toezicht. Bijvoorbeeld door het actief toepassen van gedragsinzichten en het gebruik van data-analyse. Vanuit onze expertise interpreteren wij risico's en kansen en handelen hiernaar. Dit geldt ook voor nieuwe technische ontwikkelingen waarvoor nog geen wettelijk kader is. Wij professionaliseren onze juridische kwaliteitszorg, met name op de versterking van de juridische detectie en signaleringsfunctie.

Een eigenstandige positie en reflectieve rol in het stelsel

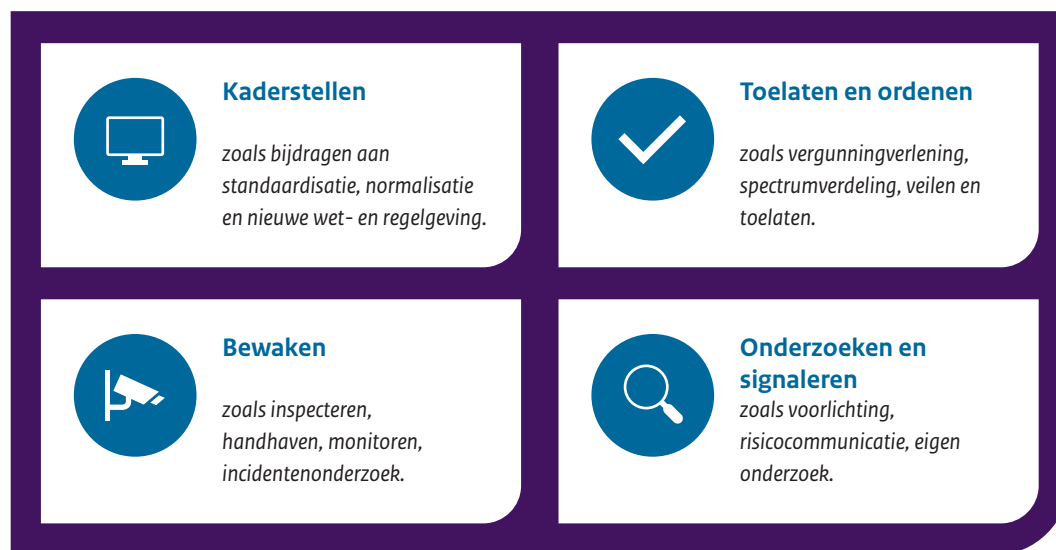
Wij reflecteren op onze positie en toegevoegde waarde en vragen hiervoor input van onze stakeholders, zodat wij ons continu kunnen verbeteren en onze dienstverlening aansluit op de behoeften van de maatschappij. Dat betekent ook dat wij actief signaleren en agenderen richting politiek en beleidsmakers over de werking van beleid en regels in de praktijk. Wij werken actief aan de verbetering van onze dienstverlening, processen en de kwaliteit van producten en diensten. Onze werkwijze is voorspelbaar, bijvoorbeeld door een groeiende inzet op openbaarmaking en transparantie van onder meer onze besluiten en beleidskaders. Daarmee dragen we bij aan bewustwording en verbetering van het vertrouwen in de digitale infrastructuur.



Met deze organisatiedoelen willen wij de risico's in onze opgaven beheersen en de maatschappelijke belangen beschermen. Het sluit aan bij de gezamenlijke inzet van de inspectieraad, het samenwerkingsverband van toezichthouders. In [het meerjarenperspectief van de Inspectieraad](#) ligt de focus op responsief toezicht met maatschappelijke oriëntatie, waarbij kwaliteitsborging, maatschappelijke verantwoording en intensieve samenwerking belangrijke pijlers zijn.

Vier kernactiviteiten

Met bovenstaande organisatiedoelen borgen en bevorderen wij de optimale inzet van de schaarse capaciteit op onze vier kernactiviteiten ten behoeve van onze maatschappelijke opgaven.





**Belangrijkste
strategische
ontwikkelingen**



Meerjarenperspectief op een hoogwaardige digitale infrastructuur

De veiligheid en beschikbaarheid van onze digitale infrastructuur zijn in het licht van wereldwijde ontwikkelingen en bijbehorende risico's allerm minst vanzelfsprekend. Deze dynamiek vraagt om een gezamenlijke, gerichte inzet. Als rijksinspectie zien wij, mede op basis van deze risico's, een duidelijke richting waarin wij samen met andere partijen willen optrekken.

Onze aanpak (zie onderstaand schema) richt zich op het stimuleren van ketenverantwoordelijkheid bij ondertoezichtgestelden, het intensiveren van samenwerking met beleid, marktpartijen en kennisinstellingen, en het tijdig positie nemen op de risico's van opkomende technologieën. Daarnaast willen wij een regierol aanbieden bij het ontwikkelen van generieke toezichtkaders, en inzetten op versterking van de algehele digitale weerbaarheid en digitale (open strategische) autonomie. Wij nemen hierin het initiatief door het gesprek aan te gaan, om samen betekenis te geven aan de ontwikkelingen en te komen tot concrete handelingsperspectieven.



Gesignaleerde ontwikkelingen

Complexiteit en verwevenheid digitale infrastructuur neemt toe

Onze omgeving is continu in beweging en vraagt een integrale stelselbenadering. Nieuwe technologieën dienen zich aan en de wet- en regelgeving wordt daarop in hoog tempo aangepast. De digitale transitie is een noodzakelijke voorwaarde voor onze digitale economie. We zien echter dat de digitale transitie en de toegenomen omvang van de digitale infrastructuur impact hebben op de Nederlandse samenleving. Wij zien daardoor veranderende maatschappelijke verwachtingen van onze rol als toezichthouder: pro-actiever en een bredere, maatschappelijke blik op de opgave. De RDI is er om in een complexe omgeving effectief de publieke belangen te beschermen.

Disruptieve technologieën en snelle acceptatie daarvan

Disruptieve technologieën zijn technologieën die werkwijzen binnen de maatschappij significant veranderen of overbodig maken; denk aan AI of Kwantum. De digitale transitie biedt kansen om onze welvaart te versterken, maar de ontwikkelingssnelheid, de schaal, de impact en de snelle acceptatie van de technologie zorgen ook voor uitdaging. Daarnaast zijn er steeds meer disruptieve omgevingsfactoren. Denk aan de geopolitieke ontwikkelingen, de digitale autonomie van Europa, de AI-wedloop met negatieve impact op verantwoord gebruik en het toegenomen belang van satellietcommunicatie.



Geopolitieke spanningen en een fragmenterende wereldorde

De verwachtingen van de digitale infrastructuur en het toezicht is onverminderd hoog. Met de toename van geopolitieke spanningen en een fragmenterende wereldorde, is de internationale veiligheid verslechterd en neemt de aanvalsoppervlakte – dat wil zeggen alle punten waarop een systeem, netwerk, product of software kwetsbaar is voor digitale aanvallen – navenant toe. In het licht van hybride en militaire dreiging, is het nodig als maatschappij voorbereid te zijn en veerkracht te kunnen tonen als de dreiging werkelijkheid zou worden. Wij zullen gezamenlijk [de weerbaarheidsopgave voor Nederland](#) moeten verdiepen en uitwerken, want een (digitaal) weerbare samenleving maken we samen.

Ook moet de RDI, zoals ook de Wetenschappelijke Raad voor het Regeringsbeleid onderstreept in haar [rapport Nederland in een fragmenterende wereldorde](#), voortdurend aandacht houden voor de genoemde ontwikkelingen en het effect ervan op de veiligheid van digitale infrastructuur.

Maatschappelijke risico's

Ketenafhankelijkheid door toename toeleveranciers

De digitale infrastructuur vormt het zenuwstelsel van onze moderne digitale samenleving. We zien steeds sterkere vervlechting door digitalisering van belangrijke maatschappelijke processen, zoals zorg, veiligheid, mobiliteit, toegankelijkheid, etc. Ook in de keten zien we steeds meer toeleveranciers van cruciale elementen voor de veilige werking van de infrastructuur. Dit leidt tot nieuwe risico's en maakt de impact van eventuele verstoringen nog minder voorspelbaar.

Ongecontroleerde import van digitale producten en gebruik in kritische omgevingen

Een bijkomende complicatie is de hoge omloopsnelheid en ongecontroleerde import (e-commerce) van digitale producten, waarbij commercieel verkrijgbare producten eenvoudig in kritische omgevingen gebruikt kunnen worden. Ook de gevolgen van (het ontbreken van) software-updates op de veilige werking van producten voegen extra onzekerheden of zwaktes toe aan het stelsel.

Wet- en regelgeving loopt achter op snelheid ontwikkelingen

Hoewel wij zien dat de wet- en regelgeving in hoog tempo wordt aangepast aan de nieuwe technologieën, zien we ook dat het proces van wetgeving en de implementatie daarvan voortdurend achterloopt op de snelheid van deze ontwikkelingen. Maatschappelijke acceptatie en gebruik van technologieën lopen zodoende voor op de regulering ervan, waardoor er onzekerheden zijn over de impact van het ongereguleerd gebruik van nieuwe technologieën op de weerbaarheid van het stelsel.

Hybride dreigingen en cloudopslag buiten Europa, bij een fragmenterende wereldorde

Diverse ontwikkelingen rakend aan ons werkveld van de digitale infrastructuur kunnen een negatief effect hebben op een “veilig verbonden Nederland”. Het gaat dan bijvoorbeeld om (hybride) dreigingen met langdurige uitval, schaarste en verstoringen, cloudopslag buiten Europa, invloed van grote Tech bedrijven, (dreigende) handelsoorlog, spionage, sabotage aan bijvoorbeeld zeekabels of de AI-wedloop met negatieve impact op verantwoord gebruik.

Waar wij in gezamenlijkheid op willen inzetten

Op basis van de hierboven beschreven ontwikkelingen en de daarbij behorende risico's nemen wij het initiatief om in gesprek te gaan met andere toezichthouders, ketenpartners, beleids- en kennisinstellingen. Samen willen wij betekenis geven aan de geschetste ontwikkelingen en de hieronder door ons voorgestelde richting verder vertalen naar concrete handelingsperspectieven.

Stimuleren van bedrijven en instellingen om verantwoordelijkheid te nemen voor de gehele keten

Niet alleen ondertoezichtgestelden, maar ook andere partijen hebben invloed op de weerbaarheid van de digitale infrastructuur, zoals marktpartijen en toeleveranciers. Deze vallen regelmatig (nog) niet onder ons toezicht. Wij spreken daarom als toezichthouder de bedrijven en instellingen aan die wel onder ons toezicht vallen en stimuleren hen om hun verantwoordelijkheid te nemen voor de keten en toeleveranciers. Zo maken



we ondertoezichtgestelden duidelijk dat digitale weerbaarheid een eigenschap is van het stelsel als geheel. Die meer is dan de som van de weerbaarheid van individuele partijen. Het is belangrijk dat ze de risico's binnen hun keten goed in beeld hebben en beheersen, waarbij digitale autonomie een belangrijk element is.

Dialogoog en samenwerking met beleid, toezichthouders, kennisinstellingen en markt over ontwikkeling en risico's

Om onze digitale infrastructuur te beschermen is het van belang dat we ons verbinden en samenwerken met kennisinstellingen en marktpartijen, de sector, maar ook met beleidsmakers en andere toezichthouders om onze opgave te realiseren. Daarnaast wordt bij regelgeving steeds vaker gekozen voor open normen om de veranderlijkheid van technologische ontwikkelingen het hoofd te bieden. De digitale infrastructuur is steeds meer verweven en vele partijen zijn daar onderdeel van. Daarnaast doorkruisen digitale diensten steeds vaker meerdere beleidsterreinen. Een voorbeeld waar de dialoog belangrijk is, zien wij bij het toenemende belang van satellietcommunicatie en de groeiende markt. Dit vraagt om focus. Eerst in de vorm van verdere verkenning en duiding en in latere fase mogelijk gevolgd door extra inzet op het gebied van satellietcommunicatie.

Vooruitlopend op regulering signaleren en agenderen en gezamenlijk met andere toezichthouders positie nemen

Als toezichthouder staan wij, samen met betrokken beleidsdepartementen, voor extra uitdagingen door de snelle opkomst van disruptieve ontwikkelingen en hun snelle maatschappelijke acceptatie. Om deze ontwikkelingen het hoofd te bieden, is netwerksamenwerking essentieel. De RDI moet vroegtijdig kunnen anticiperen op nieuwe maatschappelijke en technologische ontwikkelingen en regelgeving, juist om publieke belangen en een gelijk speelveld tussen marktpartijen (level playing field) op de juiste wijze te kunnen blijven beschermen. Wij zullen als toezichthouder een proactieve houding moeten aannemen. We willen vroegtijdig de dialoog aangaan met alle betrokkenen over de implicaties en risico's van zo'n disruptieve ontwikkeling en steeds meer met andere (Europese) toezichthouders gezamenlijk positie nemen. Vanuit die positie kunnen wij guidance geven aan de markt, ook als de wetgeving of de implementatie daarvan nog niet is afgerond.

Aanbieden regierol op overkoepelende generieke toezichtkaders en samenwerkingsarrangementen

De digitale infrastructuur ontwikkelt zich naar hyperverbonden ecosystemen en een steeds grotere integratie van platformen, digitale diensten of toepassingen, data, software en producten. Het wordt steeds belangrijker om een goede afstemming te hebben over een meerjarige benadering richting de sector, alsook over de rollen, verantwoordelijkheden en samenwerking, zowel tussen beleid en toezichthouders, als tussen toezichthouders onderling. Dit vereist een integraal beleid, waarbij de sterke afhankelijkheden tussen de verschillende onderdelen van de digitale infrastructuur steeds in het oog worden gehouden.

Vanuit onze rol als kennishouder willen wij initiatief nemen om overkoepelende generieke toezichtkaders en samenwerkingsarrangementen (bijvoorbeeld op AI) aan te bieden aan andere toezichthouders. Het vormgeven van deze generieke toezichtkaders doen we samen met andere toezichthouders. Wij zijn bereid om daarbij de regierol op te pakken.

Verhogen weerbaarheid gehele stelsel en investeren in digitale autonomie

We moeten gezamenlijk inzetten op de veiligheid van de digitale infrastructuur. Dit vraagt om scherpe economische keuzes, zoals het investeren in de Nederlandse en/of Europese, digitale autonomie. We zijn ons bewust van onze onafhankelijke positie en willen vanuit onze zelfstandigheid altijd een actueel beeld geven van de digitale weerbaarheid van de aan ons toegewezen sectoren. Wij moeten als toezichthouder het geheel kunnen overzien en willen onze expertise aanbieden waar dat de maatschappelijke opgave ten goede komt. Dit alles vraagt structureel om aandacht in het adaptief vermogen van onze organisatie. Dat vereist ook dat wij de ontwikkelingen in de huidige fase signaleren en duiden, zodat wij onze strategische focus en koers kunnen bepalen en ons paraatheidsbeleid voor de Nederlandse weerbaarheidsopgave kunnen vormgeven. Het resultaat van onze gezamenlijke inzet draagt bij aan het verhogen van de weerbaarheid van het gehele stelsel, en daarmee aan een veilig verbonden Nederland.

De focus van de RDI voor 2026





Is de infrastructuur aangelegd, verbonden en weerbaar?

Goede werking infrastructuur essentieel voor economie en samenleving

Maatschappelijke opgave

De Nederlandse samenleving rekent op een hoogwaardige analoge en digitale infrastructuur. Vanuit dat maatschappelijke belang bevordert en beschermt de RDI de beschikbaarheid van draadloze en draad gebonden netwerken en de goede werking ervan.

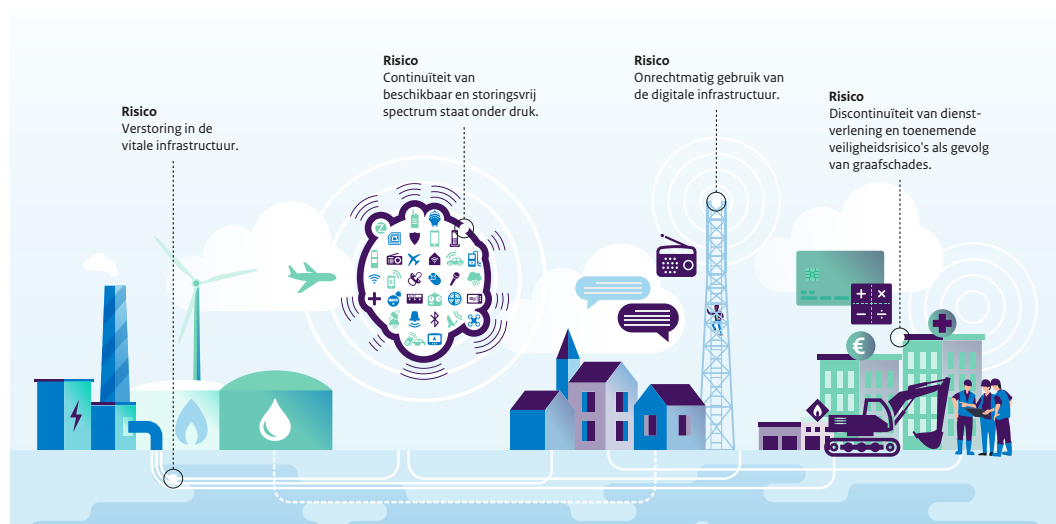
Doelen

- Optimale beschikbaarheid, dekking en capaciteit van de (digitale) infrastructuur;
- Storingsvrij gebruik van netwerken;
- Leveringszekerheid van essentiële diensten.

Resultaten

- Nederland beschikt over de voor een hoogwaardige digitale infrastructuur benodigde frequentieruimte;
- De beschikbare frequentieruimte is binnen Nederland verdeeld naar gebruikers en gebruikstoepassingen;
- De verdeelde frequentierechten zijn beschermd en de aan gegunde rechten verbonden voorwaarden worden nageleefd;
- De aanleg van kabels en leidingen in de Nederlandse ondergrond wordt zo veilig mogelijk uitgevoerd met zo min mogelijk impact op de beschikbaarheid van netwerken;
- Er is zicht op en handelingsperspectief ten aanzien van risico's en trends teneinde de beoogde doelen en resultaten ook op langere termijn zeker te stellen.

Maatschappelijke risico's met impact op resultaten



Onderbrekingen vitale infrastructuur

De geopolitieke situatie zal de komende jaren gespannen blijven. Het belang van het voorkomen van onderbrekingen in de vitale infrastructuur (zoals elektriciteit, gas, drinkwater en data) neemt daardoor toe. De beschikbaarheid van de benodigde frequentieruimte om continuïteit in een hoogwaardige digitale infrastructuur te garanderen, brengt de nodige uitdagingen met zich mee. Zo vragen steeds meer vitale toepassingen om schaarse frequentieruimte, en neemt het gebruik van technologische middelen toe die preventief of bij dreiging kunnen worden ingezet.



Veiligheidsrisico's en discontinuïteit door druk op spectrum

Spectrumbanden die vroeger druk waren zijn nu rustiger. Met de ontwikkeling van de technologie zien wij dat de wat hogere frequentiebanden drukker worden. Ook de druk op het gebruik van de ondergrond neemt de komende jaren verder toe, bijvoorbeeld door de uitrol van glasvezel en de noodzakelijke verdichting en verzwaring van de energienetten ter voorkoming van congestie. Deze druk leidt tot grotere veiligheidsrisico's, toenemende kans op storing en meer discontinuïteit van dienstverlening vanwege graafschades. Wij zetten dan ook volop in op continuïteit en storingsvrij gebruik van de netwerken in de digitale infrastructuur.

Focuspunten

Extra inspanningen in het licht van onze weerbaarheid en geopolitieke ontwikkelingen

In de opgave om Nederland veilig verbonden te houden, wordt ten gevolge van verschuivingen op het wereldtoneel ook van de RDI de nodige extra inspanningen verwacht. Zo leiden extra investeringen die worden gedaan op de infrastructuur en middelen (onder andere bij de krijgsmacht) bijvoorbeeld tot frequentie-technische inpassing. Daarnaast wordt er een zwaarder beroep gedaan op onze expertise om nieuwe technologische ontwikkelingen (storingsvrij) in te kunnen zetten ten behoeve van de veiligheid en weerbaarheid van Nederland. Ook werken wij aan aanscherping van de huidige in- en externe afspraken die gelden in het licht van 'buitengewone omstandigheden' in de Telecommunicatiewet. Op middellange termijn voorzien wij een bijdrage om uitvoering te geven aan de interministeriële agenda op het vlak van bescherming en weerbaar houden van de Nederlandse digitale infrastructuur.

Ontwikkeling van communicatienetwerken

Wij zien verschillende behoeften voor diverse toepassingen in het frequentiespectrum. Wij brengen hier onze kennis en expertise op in, zodat de (toekomstige) frequentiebehoefte bijdraagt aan de ontwikkeling van Nederland. Vanuit de driehoek bedrijfsleven–wetenschap–overheid is het Groeifondsprogramma Future Network Services (FNS)/6G opgezet, om breed innovatie te versnellen en autonomie te vergroten. In ons 6G-lab worden de nieuwste technologieën op het gebied van draadloze communicatie getest en geoptimaliseerd. Zo doen we diepgaande kennis op over nieuwe en complexe radiotechnologieën en dragen wij bij aan de ontwikkeling van de communicatienetwerken van de toekomst voor zowel burgers als bedrijven.

Satellieten en counterdrone

Op korte(re) termijn verwachten wij de radio-technische inpassing van de zogenaamde 3,8-4,2 en 26 GHz frequentiebanden. Naast de ingebruikname van nieuwe frequentieruimte zien wij ook een toename van het gebruik van satellieten. Satellietverbindingen zijn een belangrijke schakel in de beschikbaar en betrouwbaarheid van IT- en communicatienetwerken in Nederland. Vanuit het toezicht op de Wet Ruimtevaartactiviteiten (WRA) intensiveren wij het toezicht op frequentiegebruik door middel van monitoring. Op het gebied van drones vinden er op verschillende vlakken veel ontwikkelingen en onderzoeken plaats, al dan niet gekoppeld aan het voorziene frequentiegebruik. De RDI richt zich de komende periode op kaderstelling en ordening op nationaal, maar ook meer op Europees niveau. Na verloop van tijd zal daarin een verschuiving plaatsvinden richting toelating en toezicht. Met betrekking tot de inzet van counterdrone middelen zien wij een forse toename in de beoordeling en advisering met betrekking tot aanvragen. De verwachting is dat werkzaamheden op dit gebied blijven toenemen, aangezien er flink wordt geïnvesteerd op dergelijke middelen door met name de ministeries van Justitie en Veiligheid en Defensie.

Onrechtmatig gebruik van spectrum

Om een schaars goed als frequentieruimte te beschermen en continuïteit van hoogwaardige infrastructuur te waarborgen, blijven wij optreden tegen onrechtmatig gebruik van en inbreuk op het radiospectrum. Dit wordt in toenemende mate mede veroorzaakt door, weliswaar verboden, vrij verkrijgbare technologie.



Verhoging aantal inspecties in graafsector

Naast het zorgdragen voor digitale infrastructuur valt ook toezicht op het graven in de ondergrond (Wibon) onder de verantwoordelijkheid van de RDI. Sinds de start van de Wibon is het aantal graafbewegingen, mede door de uitrol van glasvezel en de energietransitie, verdubbeld tot een miljoen per jaar. Het Ministerie van Economische Zaken heeft de wettelijk voorgeschreven beleidsevaluatie verricht via een extern onderzoek. Een conclusie daaruit is dat het huidige toezicht op het zorgvuldig graven in Nederland beperkt zichtbaar is. Van belang is dat aanvullende inspectiecapaciteit wordt gevonden om de zichtbaarheid in een aantal regio's te versterken. Daarnaast ligt de focus op de meest voorkomende oorzaak van vermijdbare schade: het vooraf lokaliseren van kabels en leidingen in de ondergrond op de graaflocatie.

Aanpassingen door vorming streekomroepen

Om invulling te geven aan een evenredig verdeeld en kwalitatief goede bereikbaarheid van de omroepen draagt de RDI zorg voor een aantal verdelingen en nieuwe uitgifte van vergunningen. Zo worden in de komende jaren streekomroepen gevormd. Deze wijziging brengt de nodige aanpassingen met zich mee.



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

Samenleving vertrouwt op weerbare digitale infrastructuur

Maatschappelijke opgave

De Nederlandse samenleving rekent op de continuïteit, integriteit, vertrouwelijkheid en authenticiteit van alle dienstverlening die gebruikmaakt van die digitale infrastructuur, zodat de economie en maatschappij daar ongestoord en in vertrouwen gebruik van kunnen maken. Met ons toezicht stimuleren wij organisaties om zelf passende maatregelen te treffen. Niet alleen omdat ze daarmee voldoen aan de wetten waarop wij toezicht houden, maar ook om het volwassenheidsniveau van de digitale weerbaarheid van de eigen bedrijfsvoering te blijven verhogen. Om zo de maatschappij als geheel weerbaar te houden. Cyberaanvallen zijn niet te voorkomen en ondanks maatregelen kan een aanval leiden tot impact. Daarom zijn maatregelen nodig die zowel de kwetsbaarheden wegnemen als het herstelvermogen te vergroten. Beide onderwerpen zijn daarmee even belangrijk voor de digitale weerbaarheid. De impact van succesvolle cyberaanvallen kan immers enorm zijn. Verlies van vertrouwen in vitale diensten kan leiden tot het maatschappelijk afwijzen van digitale diensten en terugvallen op fysieke diensten waardoor zowel maatschappelijke als economische schade kan ontstaan. Onze slogan voor de introductie van onze rol als toezichthouder op de cyberbeveiligingswet is daarom: “Beveilig uw bedrijf, voor een veilig verbonden Nederland”.

Doelen

- Borgen van een betrouwbaar, waar nodig of verplicht gecertificeerd, stelsel van digitale producten, diensten en processen;
- Bewaken van een betrouwbaar stelsel of keten van middelen en diensten voor digitale identificatie en authenticatie in economie en maatschappij;
- Bewaken van de digitale weerbaarheid van vitale en essentiële dienstverleners van infrastructuur in telecom, internet en energie alsmede belangrijke (digitale) dienstverleners, zoals cloudcomputerdiensten en online marktplaatsen;
- Het onderzoeken en signaleren van ontwikkelingen in de digitale infrastructuur, het verkennen van nieuwe trends en risico's, en het informeren van maatschappij en stakeholders – zoals beleidsmakers, bedrijven en gebruikers – daarover;
- Informeren van de maatschappij over het belang van de eigen digitale weerbaarheid ten aanzien van de restrycto's die er altijd zijn.

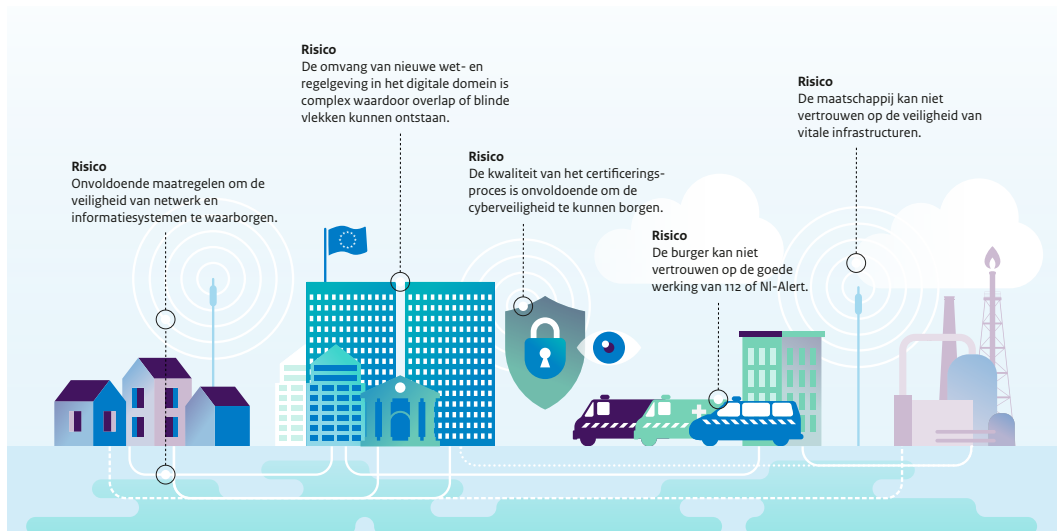
Resultaten

Met onze inspecties creëren we een gedegen beeld over de mate van weerbaarheid van de relevante sectoren. Op basis van dit beeld zetten we in op het geven van guidance, het bevorderen van de spontane naleving of het inzetten van handhaving;

- Wij laten partijen of diensten toe, na een toelatingstoets, tot de relevante stelsels;
- Wij werken actief samen met andere toezichthouders, uitvoeringsorganisaties en andere stakeholders op zowel nationaal als internationaal vlak;
- Vanuit onze werkvelden dragen wij bij aan ontwikkeling en beheer van (Europese) certificeringsschema's en de processen rond standaardisatie van cybersecurity en digitalisering;
- Er is zicht op en handelingsperspectief ten aanzien van risico's en trends om de beoogde doelen en resultaten ook op langere termijn zeker te stellen. Waar nodig is het kerndepartement geadviseerd over nieuwe of bestaande wet- en regelgeving.



Maatschappelijke risico's met impact op resultaten



Toenemende digitale dreiging vraagt om meer maatregelen

De maatschappij moet erop kunnen vertrouwen dat de weerbaarheid van de digitale infrastructuur gewaarborgd is. In de huidige tijd, met toenemende geopolitieke spanning en een meer en steeds intensiever gebruik van digitalisering als oplossing voor maatschappelijke vraagstukken, is de weerbaarheid van de digitale infrastructuur van steeds groter belang. Organisaties en bedrijven moeten eerder, steviger en meer maatregelen nemen om de toenemende digitale dreiging aan te kunnen. Met ons toezicht zetten wij in op het toetsen van die inzet en stimuleren wij het nemen van de passende maatregelen.

Complexe ketens met overlap of blinde vlekken

Om digitalisering mogelijk te maken wordt steeds vaker een complexe keten van leveranciers ingezet. Daarmee is het niet altijd direct duidelijk wat de impact van een incident in die keten voor de maatschappij betekent. De verwevenheid van componenten maakt dat een incident bij een relatief onbekende partij tot grote impact kan leiden. Dit vraagt om goed zicht op de toeleveringsketens en het in gezamenlijkheid ontdekken en onderkennen van deze verwevenheid.

Daarnaast willen wij initiatieven vanuit beleid en/of de markt stimuleren waarbij vanuit de ketens samengewerkt wordt om risico's in beeld te brengen en te beheersen. Bijvoorbeeld het Field Lab Energy Cyber Security (FLECC) waarbij op cyberbeveiligingsproblemen gefocust wordt in de offshore windindustrie op de Noordzee. Wetgeving in het digitale domein is volop in ontwikkeling. Zowel Europees als nationaal. Er lopen veel trajecten gelijktijdig waardoor een complex geheel van bestaande en nieuwe wetgeving ontstaat. Die complexiteit heeft het risico in zich dat blinde vlekken of overlap gecreëerd wordt. De RDI streeft ernaar die risico's te mitigeren door deelname en kennisdeling in het voortraject en door actieve samenwerking te organiseren in de uitvoering van toezicht op deze regelgeving.

Focuspunten

Nieuwe wetgeving leidt tot toezicht op breder scala organisaties

Het jaar 2026 staat in het teken van de inwerkingtreding van de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten en de start van de uitvoering van het toezicht daarop. Dat vraagt van ons dat wij toezicht gaan houden op een breder scala van organisaties waar we deels geen bestaande toezichtrelatie mee hebben, waaronder de sector overheid. In 2026 zetten wij in op beeldvormen en waar mogelijk kennismaken met de organisaties die we nog niet kennen. Daarnaast starten wij met opbouwen van een eerste beeld hoe het gesteld is met de weerbaarheid van de essentiële entiteiten die actief zijn in de sectoren die onder het toezicht RDI vallen. Wij brengen de belangrijkste risico's op systeemniveau in beeld om het toezicht in de jaren daarna risicogericht uit te kunnen voeren.



Voor de sector overheid hebben wij gekozen om met ons toezicht in te zetten op de kwaliteit van de verantwoordingsrapportages met betrekking tot informatiebeveiliging. Organisaties die proactief en met voldoende kwaliteit en diepgang rapporteren over de staat van hun informatiebeveiliging zullen uit die verplichting naar verwachting voldoende druk ervaren om passende maatregelen te treffen.

Voorlichting over nieuwe cyberwetgeving

Onze taak is om organisaties die met de nieuwe wetgeving te maken krijgen te ondersteunen door hen daarover te informeren en te onderzoeken in hoeverre zij al maatregelen hebben getroffen. Wij zorgen in publiek-private samenwerking via rondetafels en via congressen ervoor dat we nauw aangesloten blijven bij onze doelgroepen. Daarnaast werken wij aan de hand van guidance-producten zoals handreikingen aan efficiënte en effectieve interactie met de organisaties die onder ons toezicht staan. Zij zijn daardoor beter in staat wet- en regelgeving te vertalen naar hun praktijk. En wij als toezichthouder staan open om zo feedback op die wet- en regelgeving te ontvangen. Dit helpt de digitale weerbaarheid van Nederland ook wendbaar te organiseren.

Verhoogd belang digitale weerbaarheid

Door geopolitieke ontwikkelingen neemt het belang van een stevige toezichtrol op de digitale weerbaarheid toe. Andere nieuwe wetgeving – met bijbehorend toezicht – plaatst ons ook meer in het hart van digitale weerbaarheid. Zo leiden nieuwe certificeringsschema's onder de Cyber Security Act tot meer verzoeken aan ons als efficiënte certificerende instelling. En de ontwikkelingen op het gebied van elektronische identiteiten en vertrouwensdiensten die vorm krijgen in de eIDAS2-verordening, hebben een vergelijkbare impact.

Nieuwe regels vragen om het herijken van onze aanpak in het toezicht op bestaande partijen en om de ontwikkeling van toezicht daar waar het gaat om nieuwe diensten die onder ons toezicht gaan vallen. Daarbij richten wij ons op het zoveel mogelijk benutten van informatie die er al is. Als blijkt dat die informatie niet betrouwbaar is of als uit de informatie blijkt dat er risico's zijn, zetten wij intensievere vormen van toezicht in, zoals inspecties op locatie of andere vormen van toezicht.

Wij blijven inzetten op samenwerking met andere toezichthouders in het digitale domein. Zo hebben wij het initiatief genomen tot het inzetten op het overleg toezicht digitale weerbaarheid met alle betrokken toezichthouders op de cyberbeveiligingswet. Met dit overleg werken we aan het uniformeren van de aanpak van het toezicht om zo de toezichtslast te beperken.



Werken de producten goed en veilig?

Producten nu en in de toekomst veilig en betrouwbaar

Maatschappelijke opgave

De Nederlandse samenleving rekent op veilige en betrouwbare producten binnen de digitale en analoge infrastructuur. Wij spreken steeds meer van producten in plaats van apparaten, omdat fysieke apparaten steeds vaker software gestuurd zijn en omdat software zelf ook steeds meer een product wordt. Nederland kan erop vertrouwen dat producten onder duidelijke randvoorwaarden en volgens geldende regelgeving in de handel zijn gebracht. En dat producten storingsvrij werken, elektrisch en elektromagnetisch veilig zijn, een correcte hoeveelheidsinformatie bij handelstransacties weergeven, toegankelijk en cyberveilig zijn. Producten bevatten in toenemende mate digitale componenten. De veiligheid en betrouwbaarheid van deze digitale producten betreffen niet alleen de fysieke componenten, maar ook software, data, het gebruik van cloud en andere digitale diensten, evenals de omgeving waarin deze digitale producten gebruikt worden.

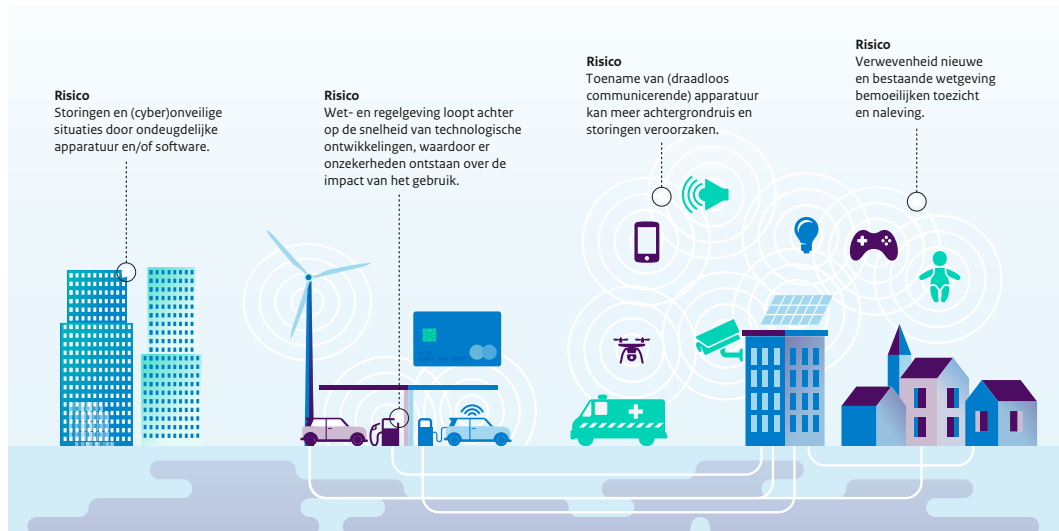
Doelen

- Kaders stellen die veilige en betrouwbare producten waarborgen. Daarbij hebben wij oog voor zowel de fysieke componenten, als de digitale componenten en de omgeving waarin deze digitale producten gebruikt worden;
- Kaders stellen die een effectieve en efficiënte spectrumverdeling en -gebruik waarborgen;
- Kaders stellen voor betrouwbare hoeveelheid- en gebruiksinformatie van producten bij handelstransacties;
- Bijdragen leveren aan het creëren van een level playing field. De voorwaarden zorgen voor gelijke spelregels voor de marktpartijen en daarmee ook voor innovatie en eerlijke concurrentie;
- Waarborgen van de kwaliteit van de digitale infrastructuur door normconform gedrag van betrokken partijen te stimuleren en te bereiken. Duidelijke voorwaarden voor het op de markt brengen en gebruik van producten geven marktpartijen de ruimte om te innoveren en eerlijk te concurreren;
- Normconform gedrag van handel in edelmetalen stimuleren en bereiken;
- Onderzoeken, signaleren en agenderen van trends, ontwikkelingen en innovaties. Advisering wet- en regelgeving kerndepartement.

Resultaten

- Eisen aan producten zijn gestandaardiseerd en genormaliseerd;
- Nederland beschikt over de benodigde internationale frequentieruimte voor gebruik;
- Nederland beschikt over een actueel Nationaal Frequentieplan, zodat stakeholders zekerheid hebben over de frequentiebestemmingen en eisen vanuit spectrumengineering;
- Storingen op frequentiegebruik door producten worden onderzocht en daar waar mogelijk en relevant weggenomen;
- Relevante wet- en regelgeving (conformiteitsregels) ten aanzien van producten wordt bewaakt en gehandhaafd;
- Relevante wet- en regelgeving ten aanzien van edelmetalen wordt bewaakt en gehandhaafd;
- Er is zicht op en handelingsperspectief ten aanzien van risico's en trends om de beoogde doelen en resultaten ook op langere termijn zeker te stellen. Waar nodig is het kerndepartement geadviseerd over nieuwe of bestaande wet- en regelgeving.

Maatschappelijke risico's met impact op resultaten



Storingen en (cyber)onveilige situaties door ondeugdelijke digitale producten

Als gevolg van de digitalisering van de maatschappij en de steeds grotere maatschappelijke afhankelijkheid van digitale producten, wordt de cyberveiligheid van hiervan steeds belangrijker. Een digitaal product dat vandaag cyberveilig is, kan morgen door een update of het ontbreken van een tijdige update, niet meer cyberveilig zijn. De sterke opkomst en invloed van AI maakt dat we op een nieuwe manier naar de veiligheid van producten moeten kijken en de omgeving waarin deze producten gebruikt worden. Om veiligheid en betrouwbaarheid van digitale producten, al dan niet met AI-componenten, te blijven borgen, is inzet op nieuw type kaders zoals geharmoniseerde standaarden en de wijze waarop we toezicht gaan houden van groot belang. Daarnaast is de veiligheid van digitale producten op de andere gebieden, zoals elektrische en elektromagnetische veiligheid, ook steeds meer afhankelijk van software, data, het gebruik van cloud en andere digitale diensten, maar ook van de omgeving waarin het product gebruikt wordt. De RDI intensificeert in 2026 het toezicht op de cyberveiligheid van digitale producten door in te zetten op het mitigeren van de risico's voor individuele gebruikers en te kijken naar risico's die grootschalige cyberaanvallen tot gevolg kunnen hebben.

Snel opkomende disruptieve technologieën en hun verwevenheid

Ontwikkelingen gaan sneller dan wet- en regelgeving. De gestage opkomst van kwantum-technologie, de dynamische ontwikkeling in digitalisering en de ontwikkeling van AI hebben naar verwachting op korte termijn verstrekkende gevolgen. In toenemende mate komen producten op de markt die zowel draadloos communiceren, digitale elementen bevatten, en ook data en AI gebruiken. Deze verwevenheid maakt het vraagstuk multidisciplinair, niet alleen binnen toezicht maar ook in relatie tot beleid en wet- en regelgeving. Om veiligheid en betrouwbaarheid van producten te blijven borgen, is inzet op trends, integrale risicoanalyse, handelingsperspectieven en een netwerksamenwerking met opdrachtgever, relevante toezichthouders en andere stakeholders noodzakelijk. Bij overlap tussen diverse wetgevingen rond digitale taken zal gewerkt worden aan integrale trendanalyse, risicoanalyse en handelingsperspectieven.

Niet acceptabele storing en risico's door toename hoeveelheid non compliant producten

Door toename van de hoeveelheid (draadloos communicerende) producten voor diverse toepassingen, neemt ook de hoeveelheid (door producten veroorzaakte) achtergrondruis en storingen toe. Een product kan voldoen aan de normen, maar bij grote aantallen producten kunnen versturende achtergrondruis (Man Made Noise) of een niet acceptabele grotere storing in het spectrum ontstaan, waardoor producten niet meer werken zoals verwacht. Dit effect wordt negatief versterkt door de toename van non-compliant producten uit landen als China die veelal direct door consumenten worden geïmporteerd. Om veiligheid en betrouwbaarheid van producten te blijven borgen, is inzet op het voorkomen van accumulatieve storing en inzet op het weren van import van ondeugdelijke producten noodzakelijk. Ontwikkelingen op het gebied



van circulaire en duurzame producten zoals EU-regelgeving onder de Eco Design richtlijn (bijvoorbeeld right to repair, batterijen, Digital Product Passport) brengen extra eisen met zich mee voor producten die ook onder de Radioapparaten-richtlijn of EMC-richtlijn vallen. Om veiligheid en betrouwbaarheid van producten te blijven borgen, is het noodzakelijk om met een brede integrale blik naar nieuwe en bestaande wetgeving te kijken. Dit kan worden bereikt door netwerksamenwerking en informatie-uitwisseling met andere betrokken toezichthouders.

Focuspunten

Coördinatie en toezicht op AI-Act

In 2026 ligt een sterke focus op de implementatie van het toezicht op de AI-act. De voorbereiding op de beoogde rol van de RDI als toezichthouder, de RDI als coördinator van toezichthouders en samenwerking met Autoriteit Persoonsgegevens, directie Coördinatie Algoritmes als beoogd toezichthouder op de AI-act, wordt afgerond en wordt naar verwachting uitgevoerd. De AI-act is een nieuwe wetgeving, met de kaders en toezichtstaken voor het gelijk speelveld van marktpartijen en veiligheid van digitale producten met AI-componenten. De beoogde toezichtstaken voor de RDI leveren een bijdrage aan een veilig verbonden Nederland. Met de beoogde rol als coördinator van toezichthouders, en de SPOC rol (singel point of contact), pakt RDI haar rol om een netwerksamenwerking vorm te geven en een toezichthouder-brede integrale blik op het stelsel te organiseren. Daarbij blijft elke toezichthouder verantwoordelijk voor toezicht binnen het eigen stelsel. Omdat AI een maatschappelijk vraagstuk is dat zich kan manifesteren in verschillende stelsels, het kan onder verschillende wet- en regelgevingen vallen, is een netwerksamenwerking noodzakelijk om te bepalen via welk stelsel het toezicht het meest effectief kan worden ingezet. Randvoorwaarde voor de RDI om toezicht op de AI-act op zich te nemen is dat de benodigde structurele middelen om verantwoord toezicht neer te zetten in voldoende mate worden toegekend.

Voorbereiding op de Cyber Resilience Act (CRA)

Daarnaast worden de voorbereidingen op het toezicht op de CRA, die in 2027 van kracht wordt, geïntensiveerd en bereidt de RDI de rol als toezichthouder voor. Ook de CRA is een nieuwe wetgeving met kaders voor het gelijke speelveld van marktpartijen, veiligheid van producten met digitale componenten, en eisen voor transparantie, die daarmee een bijdrage levert aan een veilig verbonden Nederland. Met de beoogde rol als toezichthouder op de CRA, haar leidende inzet op het gebied van standaardisatie, en haar netwerksamenwerking met (inter-)nationale collega toezichthouders, pakt RDI haar rol om een toezichthouder-brede integrale blik op het stelsel te organiseren. De RDI voert in aanloop naar het toezicht op de CRA haar toezichtstaak op het gebied van digitale veiligheid van producten vanuit de RED 3.3 d, e en f uit. Ook hier geldt als randvoorwaarde voor de RDI dat zij deze taak en verantwoordelijkheid voor een weerbaar Nederland alleen op zich kan nemen indien de benodigde structurele middelen om verantwoord toezicht neer te zetten in voldoende mate worden toegekend.

Intensivering toezicht op non-compliant e-commerce producten

Een focuspunt is ook de intensivering van het toezicht op de grote hoeveelheden non-compliant producten die via e-commerce op de Europese markt komen. De intensivering komt mede voort uit het Europese initiatief om te komen tot Priority Control Areas (PCA). E-commerce is een voorbeeld van een maatschappelijke ontwikkeling, waarbij met bestaande wet- en regelgeving geacteerd moet worden op een verandering in het gelijk speelveld tussen marktpartijen. De verandering is zodanig groot dat bestaande toezicht activiteiten ondanks intensivering, onvoldoende handvatten bieden om efficiënt en effectief toezicht te kunnen houden. De enorme toename in non-compliant producten die van buiten Europa op de Nederlandse en Europese markt komen, heeft een grote impact op de weerbaarheid en autonomie van een veilig verbonden Nederland. Zo stimuleren wij bedrijven en instellingen om verantwoordelijkheid te nemen voor de gehele keten en willen we bewustwording creëren door leidende principes voor de sector op te stellen. Zo gaan we samen met andere markttoezichthouders de Nederlandse markttoezicht strategie 2026-2030 opstellen.



Samenwerken aan een weerbare infrastructuur voor Caribisch Nederland

Maatschappelijke opgave

De digitale transitie voor Caribisch Nederland vraagt van ons dat wij vanuit onze maatschappelijke verantwoordelijkheid de beschikbaarheid van netwerken bevorderen en beschermen, het storingvrij gebruik van radioapparaten bevorderen en bijdragen aan de continuïteit en integriteit van netwerken. Daarmee geven wij uitvoering aan de maatschappelijke opgave die voortvloeit uit de Wet telecommunicatievoorzieningen BES (Bonaire, Sint-Eustatius en Saba) en onderliggende regelgeving. Zo zorgen wij voor een veilig verbonden Caribisch Nederland.

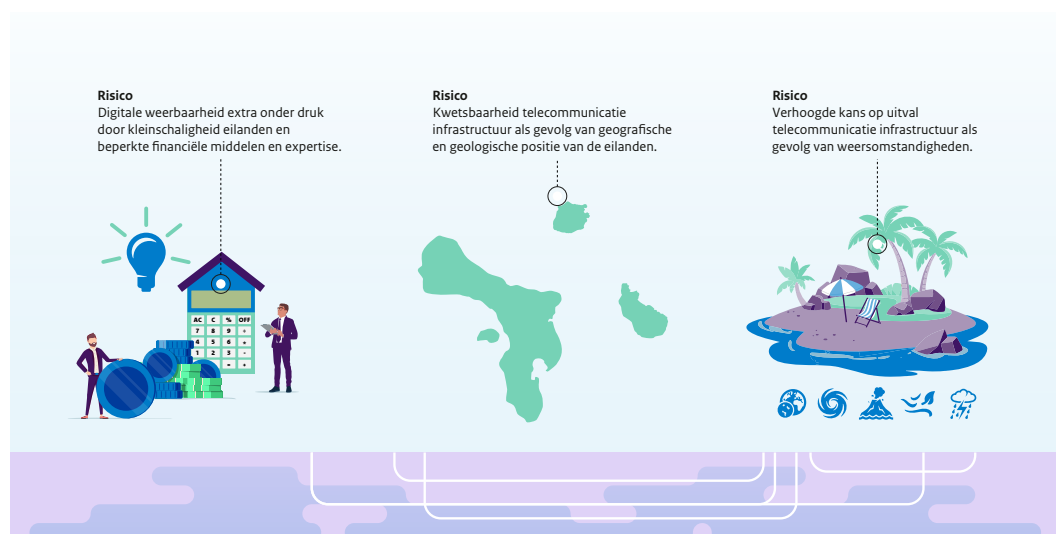
Doelen

- Optimale beschikbaarheid, dekking en capaciteit van de (digitale) infrastructuur;
- Storingvrij gebruik van netwerken en apparaten;
- Continuïteit, integriteit, vertrouwelijkheid en authenticiteit van de dienstverlening via de digitale infrastructuur.

Resultaten

- Caribisch Nederland beschikt over de frequentieruimte die nodig is voor een hoogwaardige digitale infrastructuur;
- De beschikbare frequentieruimte is binnen Caribisch Nederland verdeeld naar gebruikers en gebruikstoepassingen;
- De verdeelde frequentierechten zijn beschermd en de aan gegunde rechten verbonden voorwaarden worden nageleefd;
- Storingen op frequentiegebruik door producten worden onderzocht en daar waar mogelijk en relevant weggenomen;
- Wij werken actief samen met andere toezichthouders, uitvoeringsorganisaties en andere stakeholders op zowel nationaal als internationaal vlak;
- Ontwikkelen van kwaliteitstoezicht: de concessiehouders nemen passende technische en organisatorische maatregelen om de continuïteit van de digitale infrastructuur te waarborgen.

Maatschappelijke risico's met impact op resultaten



Risico's omtrent beschikbaarheid digitale infrastructuur door kleinschaligheid van eilanden en weersomstandigheden
Door de kleinschaligheid van de eilanden, de hierdoor beperkt aanwezige (financiële) middelen en expertise, de geografische en geologische positie van de eilanden en het klimaat (orkanen, invloed van zee en zout) kan de digitale infrastructuur op de eilanden niet vergeleken worden met de situatie in Europees Nederland.



Het bouwen, onderhouden en exploiteren van telecommunicatie-infrastructuur brengen hogere kosten met zich mee dan in Nederland. Bijvoorbeeld omdat het graven in harde rotsgrond een uitdaging is en operators te maken hebben met extra transportkosten. Daarbij moeten de opbrengsten worden terugverdiend op een relatief laag aantal abonnees.

De weersomstandigheden vormen bovendien een groter risico ten aanzien van de beschikbaarheid van de telecommunicatie-infrastructuur. Overstromingen, modderstromen, extreme windsnelheden en het zoute zeewater zorgen ervoor dat er een risico is dat telecommunicatie-infrastructuur niet altijd beschikbaar is. Dit geldt voor de gehele keten (stroomvoorziening, aanvoerlijnen over zee en in de lucht, etc.) waardoor de beschikbaarheid van telecommunicatie-infrastructuur kwetsbaar is.

Digitale weerbaarheid infrastructuur extra onder druk

In Europees Nederland gelden steeds meer (Europese) regels ten aanzien van digitale weerbaarheid. Deze regels zijn 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 is gewaarborgd.

Maatschappelijk gezien worden de onderwerpen beschikbaarheid (waaronder continuïteit), authenticiteit, vertrouwelijkheid en integriteit steeds belangrijker omdat de burgers en bedrijven in Caribisch Nederland volwaardig mee moeten en willen doen aan de digitale economie. Daarvoor is nodig dat een aantal basisvoorzieningen op orde is en blijft, waaronder een stabiele en duurzame digitale infrastructuur.

Focuspunten

Digitale weerbaarheid van Caribisch Nederland

De komende jaren zet de RDI meer in op de digitale weerbaarheid van Caribisch Nederland. Voor een betrouwbare telecommunicatie-infrastructuur moet deze afdoende worden beschermd. Om die reden worden in de concessievoorschriften maatregelen geëist om het netwerk te beschermen tegen acties die de beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit in gevaar brengen. Samen met de concessiehouders wordt invulling gegeven aan deze norm en wordt hier toezicht op gehouden. Ook zal een toezichtskader worden opgesteld, waarin wordt omschreven op welke manier de RDI toezicht zal houden op deze normen.

Daarnaast zet de RDI in op bewustwording, ook rond onderwerpen waar (nog) geen taak ligt voor de RDI, maar wel een maatschappelijke verantwoordelijkheid wordt gevoeld. Als resultaat nemen de concessie- en machtiginghouders stap voor stap passende technische en organisatorische maatregelen. Zo verkleinen zij de risico's voor zichzelf, voor de consument en voor de maatschappij in zijn geheel.

Vernieuwing wetgeving

De RDI vervult een signalerende en agenderende functie. Door de technologische ontwikkelingen van de telecominfrastructuur levert huidige wetgeving onvoldoende houvast, waardoor maatwerk nodig is. Daarnaast signaleert de RDI aan de directie Digitale Economie van het Ministerie van Economische Zaken maatschappelijke ontwikkelingen, die niet of onvoldoende in de huidige wet- en regelgeving zijn geregeld. De Directie Digitale Economie van het Ministerie van Economische Zaken is samen met de Autoriteit Consument & Markt en de RDI aan het onderzoeken waar de bestaande telecomwetgeving moet worden vernieuwd om zo beter aan te sluiten bij de huidige ontwikkelingen.

Duurzame samenwerking

De RDI werkt met een aantal organisaties samen. Met een enkele andere organisaties wordt nu verkend hoe we elkaar kunnen versterken in onze maatschappelijke opgave waar we voor staan. Dit moet de komende jaren resulteren in duurzame samenwerkingsverbanden. Hierdoor worden de schaarse kennis, expertise en middelen efficiënt en effectief benut. Dit komt het toezichthouden in zijn geheel ten goede. Het gaat daarbij om organisaties als de Douane, de Scheepvaartinspectie, het Commissariaat voor de Media, Openbare Lichamen, Digital Trust Center, Nationaal Cyber Security Center, de Kamer van Koophandel en visserijorganisaties.



De RDI als organisatie in beeld



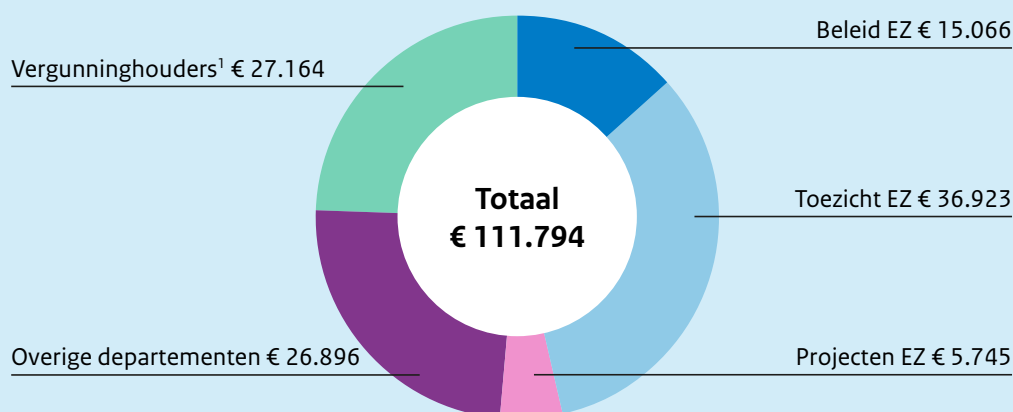
Organisatiecijfers

De Rijksinspectie Digitale Infrastructuur valt als rijksinspectie onder de verantwoordelijkheid van de Minister van Economische Zaken. Als toezichthouder werkt de RDI sectoroverstijgend in opdracht van verschillende ministeries, zoals het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het Ministerie van Justitie en Veiligheid en het Ministerie van Klimaat en Groene Groei. Deze brede verantwoordelijkheid vraagt om een integrale aanpak van toezicht op de digitale infrastructuur van Nederland.

Onze begroting voor 2026

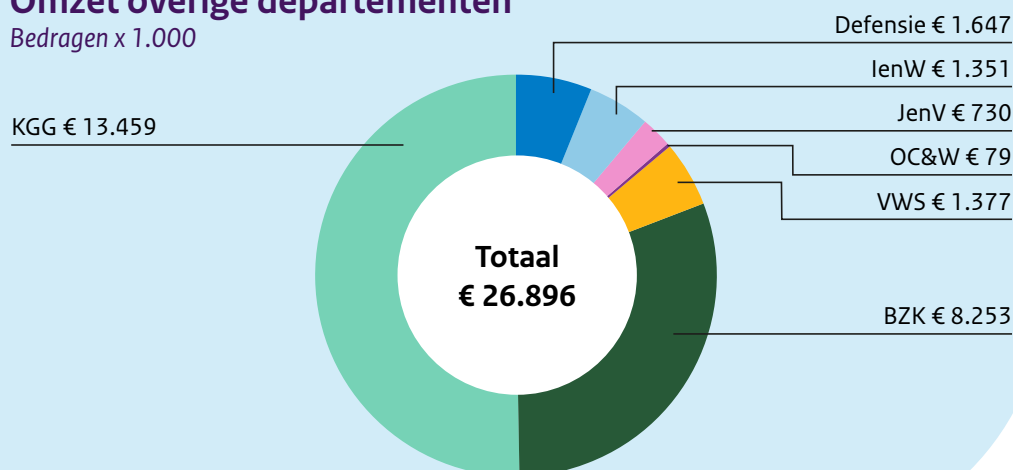
Omzet RDI 2026

Bedragen x 1.000



Omzet overige departementen²

Bedragen x 1.000

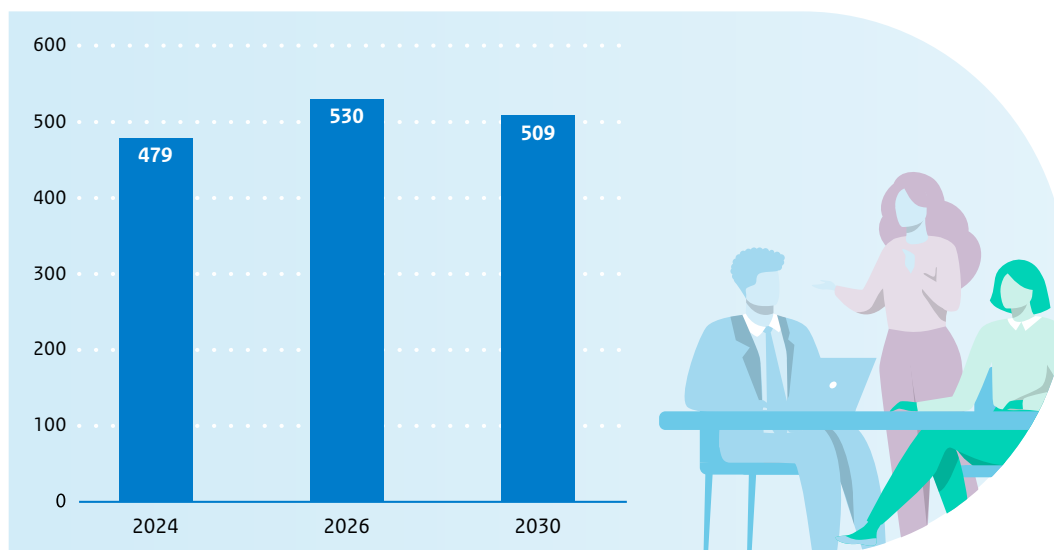


1: Betreft uitgifte vergunningen voor mobiele verbindingen, tijdelijke verbinden, marifoongebruik en/of radiozendamateurs.

2: Betreft inkomsten uit vergunningen ten behoeve van het gebruik van een specifiek, beschermd deel van het frequentiespectrum en toezichtsoverdrachten bij BZK en KGG.



RDI in Fte's



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

Emmasingel 1 Groningen

088 - 041 60 00

info@rdi.nl

www.rdi.nl

Oktober 2025



#wijzijnRDI