Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Verantwoord verweven?

Publieke belangen onder druk door complexe ecosystemen en ketenafhankelijkheden

Meerjarenplan 2025-2029

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

Inhoud

De Inspecteur-Generaal aan het woord

Netwerksamenwerking cruciaal om publieke belangen te dienen

Voor u ligt ons meerjarenplan, dat tot stand is gekomen in een context van de veranderende digitale infrastructuur en waarin de ontwikkelingen meer en meer met elkaar verweven raken. De snelheid waarmee de disruptieve technologieën elkaar opvolgen en de complexiteit van de verschillende ecosystemen vragen van ons een meerjarige inspanning om de publieke belangen te dienen. Daarnaast is wendbaarheid belangrijk om op de actualiteiten in te kunnen spelen en onze maatschappelijke verantwoordelijkheid te nemen.

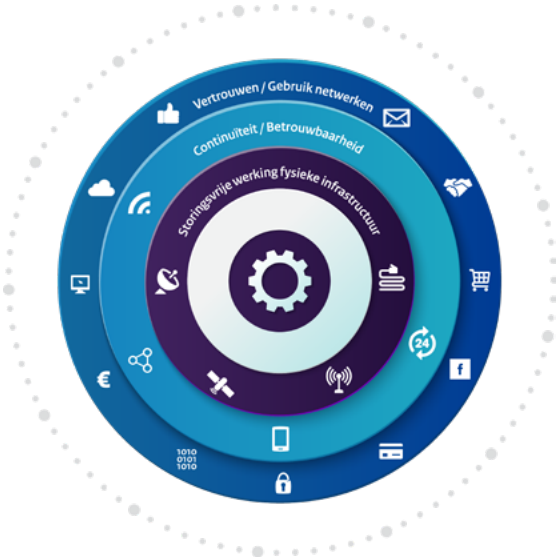
De digitale transitie biedt kansen om onze welvaart te versterken en is een noodzakelijke voorwaarde voor de energietransitie. De digitale transitie brengt echter ook risico's met zich mee, zeker in tijden van geopolitieke spanningen. Zo maakt de toenemende afhankelijkheid van de digitale infrastructuur ons kwetsbaar voor uitval en verstoringen, bijvoorbeeld als gevolg van cyberaanvallen of menselijke fouten. Om deze risico's te beperken zonder afbreuk te doen aan de kansen die de digitale transitie biedt, wordt op mondiaal en Europees niveau hard gewerkt aan noodzakelijke regulering.

Zowel de regulering als de digitale transitie zelf vragen van het toezicht een nieuwe benadering. Want enerzijds kenmerkt de digitale transitie zich door een grote technologische complexiteit en een hoge snelheid waarmee innovaties als AI en quantumtechnologie hun toepassing vinden. Anderzijds voltrekt de digitale transitie zich in de volle breedte van economie en samenleving. Deze ontwikkelingen hebben impact op de maatschappelijke opgaven, het werkveld en de werkwijze van ons als rijksinspectie om de risico's in de samenleving te mitigeren. Gezien het toegenomen belang van digitale infrastructuur heeft de RDI de afgelopen jaren een noodzakelijke ontwikkeling doorgemaakt. Zowel onze opgave, onze opdrachtgevers als omvang zijn toegenomen om tegemoet te komen aan de opdracht een veilig verbonden Nederland te waarborgen.

De ontwikkelingen vragen om netwerksamenwerking waarbij kracht, inzet en expertise gebundeld wordt. Bijvoorbeeld met ministeries, publieke en private partijen, het opstellen van de Nederlandse cybersecuritystrategie en gezamenlijk met stakeholders de regeldruk op ondertoezichtgestelden bewaken. Ook de samenwerking met andere toezichthouders via de Inspectieraad en het Samenwerkingsplatform Digitale Toezichthouders speelt een belangrijke rol om de effectiviteit en maatschappelijke positie van toezichthouders te vergroten.

We presenteren u ons meerjarenplan waarbij we ingaan op de risico's die we zien en de focus die we leggen om een veilig verbonden Nederland te kunnen waarborgen. In dit meerjarenplan besteden we allereerst aandacht aan de inrichting van ons toezicht om klaar te zijn voor de toekomst. Vervolgens beschrijven we de meerjarige ontwikkeling die we zien en waar we onze aandacht op richten. Tot slot geven we de focus aan voor het komende jaar.

Onze maatschappelijke opgave is een veilig verbonden Nederland, zodat Nederland kan vertrouwen op de beschikbaarheid van de digitale infrastructuur, die continu en veilig te gebruiken is. 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?

De samenleving moet erop kunnen vertrouwen dat wij maatschappelijke vraagstukken rond de digitale infrastructuur tijdig detecteren, risico's signaleren en belangen beschermen. Dit is noodzakelijk voor de betrouwbaarheid van en vertrouwen in de digitale infrastructuur. We hebben een maatschappelijke oriëntatie en een proactieve houding richting burgers, instellingen en bedrijven. We luisteren en reageren op signalen uit de samenleving en hebben oog voor de verschillende meningen en belangen. Op deze manier staan we samen voor de digitale infrastructuur en ontwikkelen we door om Nederland veilig verbonden houden.

Angeline van Dijk
Inspecteur-Generaal Rijksinspectie Digitale Infrastructuur

Hoe wij werken als RDI

Als organisatie klaar voor de opgaven van de toekomst

Het belang van de digitale infrastructuur groeit en synchroon daaraan groeit de organisatie van de Rijksinspectie Digitale Infrastructuur (RDI) mee; grotere complexiteit, meer regels om op toe te zien, nieuwe stakeholders en ondertoezichtgestelden (OTG's). Om vorm te geven aan hoe wij ons toezicht inrichten heeft de RDI een drietal (strategische) organisatiedoelen geformuleerd:

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

Een informatiegestuurde & risicogerichte benadering staat centraal in ons werk

Een eigenstandige positie & reflectieve rol in het stelsel

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

We kennen het stelsel en de spelers zodat we 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. We blijven onderzoek doen om onze kennis te vergroten en delen deze resultaten met onze stakeholders.

Een informatiegestuurde & risicogerichte benadering staat centraal in ons werk

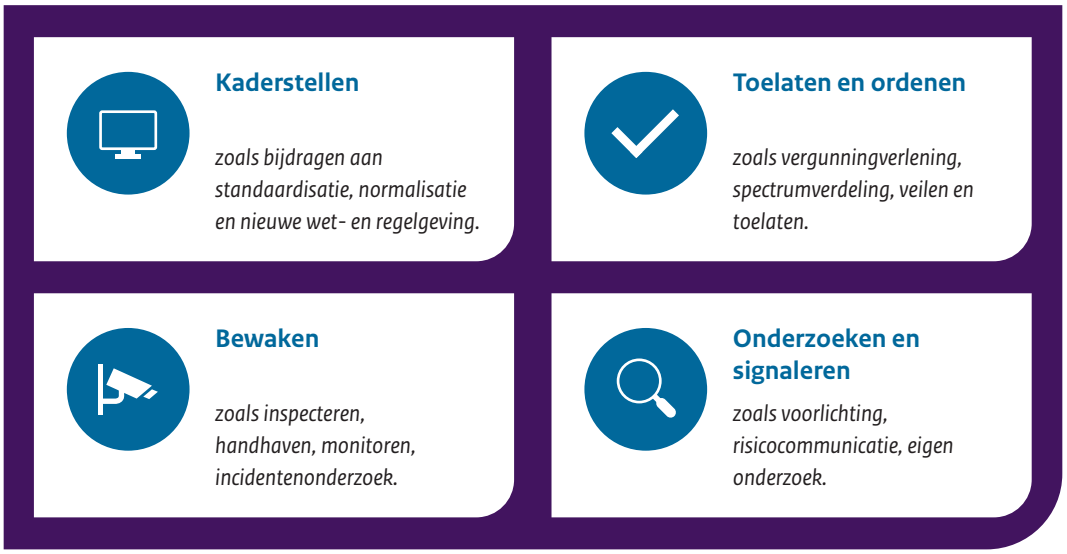
We hebben zicht op kansen en risico's in de digitale infrastructuur, zitten aan de 'voorkant' en zijn betrokken bij (internationale) beleidsvorming en regelgeving. We verkennen actief technologische en maatschappelijke ontwikkelingen en blijven inzetten op het verder ontwikkelen van onze informatiegestuurde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

Een eigenstandige positie & reflectieve rol in het stelsel

We reflecteren op onze positie en toegevoegde waarde en vragen hierin input van onze stakeholders, zodat we ons continu kunnen verbeteren en onze dienstverlening aansluit op de behoeften van de maatschappij. Dat betekent ook dat we actief signaleren en agenderen richting politiek en beleidsmakers over de werking van beleid en regels in de praktijk. We 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.

Kernactiviteiten

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



Belangrijkste strategische ontwikkelingen

Meerjarenperspectief op een hoogwaardige digitale infrastructuur

We staan er als Rijksinspectie Digitale Infrastructuur (RDI) voor om in een complexe omgeving effectief de publieke belangen te kunnen beschermen. Nieuwe technologieën dienen zich aan, de wet- en regelgeving wordt daarop aangepast en tegelijkertijd is het vertrouwen in de digitale infrastructuur hoog. Wij bereiden ons graag vroegtijdig voor op deze nieuwe ontwikkelingen, juist om deze publieke belangen op de juiste wijze te beschermen. Denk bijvoorbeeld aan de energietransitie, waarbij een hoogwaardige digitale infrastructuur randvoorwaardelijk is. Tegelijkertijd zien we ook een verschuiving in het toezichtlandschap, die een andere werkwijze vraagt van toezichthouders. We schetsen in dit hoofdstuk een aantal ontwikkelingen die wij zien en hoe we hier de komende jaren op willen acteren.

Netwerksamenwerking is cruciaal voor het toezichtstelsel

Netwerksamenwerking komt tot uitdrukking in zowel de beleidssamenwerking met departementen als in ons internationale speelveld. Eveneens werken we intensief samen met marktpartijen, zoals telecomproviders of fabrikanten. Het is noodzaak om als toezichthouder het geheel te blijven zien en te coördineren, beheren en onze expertise aan te bieden. Deze samenwerking en de toename van regelgeving is sectoroverstijgend. De overlap tussen de onderlinge beleidsdepartementen en toezichthouders kent een complex speelveld aan belangen.

Het is binnen de digitale infrastructuur belangrijk om een goede afstemming te hebben over rollen, verantwoordelijkheden en samenwerking tussen zowel beleid en toezichthouders als toezichthouders onderling. We zien hierbij een rol voor ons waarbij we initiatief willen nemen om overkoepelende generieke toezichtkaders te bieden die behulpzaam zijn voor andere toezichthouders om hun zelfstandige rol te kunnen uitvoeren. Het vormgeven van deze generieke toezichtkaders doen we graag in gezamenlijkheid met de andere toezichthouders. Vanuit deze generieke kaders en de samenwerking met toezichthouders zijn we bereid om de regierol op te pakken. Ook bieden we hulp aan andere toezichthouders vanuit onze technische expertise.

Bij deze samenwerking zijn we ons bewust van onze onafhankelijke positie en de positie van de anderen en zorgen dat we die met elkaar borgen. We definiëren gezamenlijk wat we verstaan onder toezichthouden en kiezen voor een meerjarige benadering richting de sector. We zorgen zodoende voor heldere verwachtingen die we delen met onze netwerkpartners. Zo borgen we eenduidigheid binnen het digitale domein, maar wel vanuit ieders eigen positie. Naast deze samenwerking zullen we natuurlijk vanuit onze zelfstandigheid altijd een actueel beeld geven van de digitale weerbaarheid van de aan ons toegewezen sectoren.

Verwevenheid van disruptieve technologieën

Disruptieve technologieën zijn technologieën die werkwijzen binnen de maatschappij significant veranderen of overbodig maken. De ontwikkelingssnelheid, de schaal en de impact van de technologie zorgen ook voor uitdaging, gezien de veiligheid en continuïteit van de digitale infrastructuur en digitale samenleving. We zien dat dit gepaard gaat met exponentiële groei van digitale producten en diensten, met grote impact in de digitale samenleving.

Als toezichthouder staan we voor uitdagingen door de snelle opkomst van disruptieve ontwikkelingen. Maatschappelijke acceptatie en gebruik lopen voor op de regulering ervan. Regelgeving kiest steeds vaker voor open normen om de veranderlijkheid van technologische ontwikkelingen het hoofd te bieden. Dit betekent dat invulling hiervan via standaardisatie en wetgeving achterloopt op het moment dat de risico's in de digitale infrastructuur ontstaan.

De belangrijkste disruptieve technologieën van dit moment:

Kunstmatige intelligentie (AI)
Er wordt door onze ondertoezichtgestelden steeds meer gebruik gemaakt van AI, in de digitale infrastructuur, maar ook in steeds meer toepassingen die werken op of in deze digitale infrastructuur. De ontwikkelingen hierin gaan razendsnel, dankzij de explosieve ontwikkeling van Large Language Modellen (LLM). Er is een investering op kennis en vaardigheden nodig om de impact van deze technologie op lange termijn te kunnen duiden. Om het gebruik van AI in goede banen te leiden moet bewaakt worden dat AI betrouwbaar en vertrouwenswaardig wordt toegepast in het digitale domein.

Quantumtechnologie
Quantumtechnologie staat nog voor een doorbraakmoment, maar er wordt steeds meer bekend over de mogelijke impact. Nieuwe cryptografische mechanismen (post-quantum cryptografie, PQC) moeten in gebruik worden genomen, voordat quantum computing beschikbaar is. Want met een quantum computer kunnen de huidige mechanismen gekraakt worden: geheimen zijn dan niet meer digitaal veilig. Dit gaat grote gevolgen hebben voor de veiligheid van onze digitale infrastructuur.

Dit vraagt van ons als toezichthouder een proactieve houding, waarbij ook in de fase van onzekerheid al dialoog moet plaatsvinden over de mogelijke implicaties en risico's van zo'n disruptieve technologie.

Steeds vaker wordt van een toezichthouder verwacht om vooruitlopend op regulering al voor te sorteren op ontwikkelingen en die te beïnvloeden. Dit vraagt om een structurele investering in het adaptief vermogen van onze organisatie. Hier ligt, vanuit een gezamenlijke verantwoordelijkheid, voor ons als Rijksinspectie, samen met de beleidskern, een actieve opgave om vroegtijdig te signaleren welke kansen gestimuleerd worden en welke risico's juist moeten worden gemitigeerd. We zetten meerjarig in op innovatie en het verder ontwikkelen van kennis en werkwijzen. Daarnaast participeren we in Europese en nationale netwerken om kennisontwikkeling, kennisdeling en standaardisatie te stimuleren op het thema digitale weerbaarheid.

Complexe ecosystemen en ketenafhankelijkheden

De digitale infrastructuur ontwikkelt zich naar hyperverbonden ecosystemen en een steeds grotere integratie van apparaten, toepassingen en verbindingen. Een voorbeeld is de twin transition waarbij de digitale en energiesystemen integreren en waarbij systemen steeds meer decentraal opereren. Deze verweving speelt ook voor de digitale sector, zoals de nieuwe netwerk- en informatiesystemen richtlijn (NIS2). Deze richtlijn wordt in Nederland vertaald in de Cyberbeveiligingswet, waarvan de verwachting is dat deze wet in 2025 ingaat. In algemene zin zien we sterkere vervlechting door digitalisering van belangrijke maatschappelijke processen, zoals zorg, veiligheid, mobiliteit etc. Ook in de keten zien we steeds meer toeleveranciers van cruciale elementen voor de veilige werking van de infrastructuur. Een bijkomende complicatie is de hoge omloopsnelheid en grote volumes van (nieuwe) apparatuur. Ook de gevolgen van software en applicatie-updates op de functionaliteiten van producten voegen extra complexiteit toe aan het stelsel. Zoals blijkt uit de Strategie Digitale Economie van het ministerie van Economische Zaken vergt dit veel van alle onderdelen van de digitale infrastructuur, waarbij steeds bewaakt moet worden dat er geen zwakke schakels ontstaan die het geheel afremmen. Dit vereist een integraal beleid, waarbij de sterke afhankelijkheden tussen de verschillende onderdelen van de digitale infrastructuur steeds in het oog worden gehouden en waar schaarse middelen zoals spectrum op een doelmatige wijze worden verdeeld.

Doordat essentiële digitale diensten afhankelijk zijn van dit complexe ecosysteem is er steeds vaker sprake van aanvankelijk geïsoleerde risico's die uiteindelijk doorsijpelen naar het totale stelsel en zo een groot risico vormen voor veilige en weerbare gebruikers. Het ecosysteem is steeds minder overzichtelijk en met name de invloed en rol van derde partijen binnen deze systemen vormen een risico voor de weerbaarheid van het totale stelsel.

Niet alleen ondertoezichtgestelden, maar ook andere partijen hebben invloed op de weerbaarheid van de digitale infrastructuur, zoals toeleveranciers. Deze vallen regelmatig niet onder ons toezicht. We spreken daarom als toezichthouder de bedrijven en instellingen die wel onder ons toezicht vallen aan en stimuleren hen om hun verantwoordelijkheid te nemen voor de keten en toeleveranciers. Daarnaast zullen we inzetten op gedragsbeïnvloeding en vergroten van bewustwording. Guidance kan als instrument meewerken aan een veilig verbonden Nederland en zullen we doorontwikkelen en breder inzetten. Hiervoor voeren we onderzoek uit naar een passend kader voor guidance dat kan worden toegepast in de toezichtsdomeinen van de RDI. Wij geloven dat de digitale weerbaarheid van organisaties van cruciaal belang is voor het vertrouwen in een digitale samenleving en economie. Zo dragen wij bij aan een veilig verbonden Nederland.

Moderne kaders zijn nodig in Caribisch Nederland

De ontwikkelingen in Caribisch Nederland gaan langzamer dan in Europees Nederland, maar de verschillen worden op termijn kleiner. De verwachting is dat de bevolking van Bonaire behoorlijk groeit en ook het aantal elektronische zend- en ontvangapparaten blijft groeien. Daarom is het van belang om op de risico's te blijven inzetten, zodat de beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit van de digitale infrastructuur wordt gewaarborgd.

De huidige wet- en regelgeving in Caribisch Nederland gaat al meer dan 30 jaar mee (enkele aanpassingen daargelaten). De maatschappelijke ontwikkelingen, bijvoorbeeld ten aanzien van de afhankelijkheid van zeekabels, nieuwe vormen van telecommunicatie zoals satellietcommunicatie, de toegenomen handel in elektronische apparaten, de duurzaamheid van de infrastructuur en de noodzaak van cyberveiligheid, vragen om een herijking van het telecomkader.

In Caribisch Nederland ligt onze meerjarige inzet op:
- Vernieuwen bestaande wetgeving & aansluiten op nieuwe wetgeving (comply or explain);
- Uitvoeringskracht vergroten (samenwerken en werven (tijdelijk) personeel);
- Voorbereiding nieuwe taken;
- Onderzoeken, monitoren en acteren op nieuwe ontwikkelingen Caribisch Nederland.

De focus van RDI voor 2025

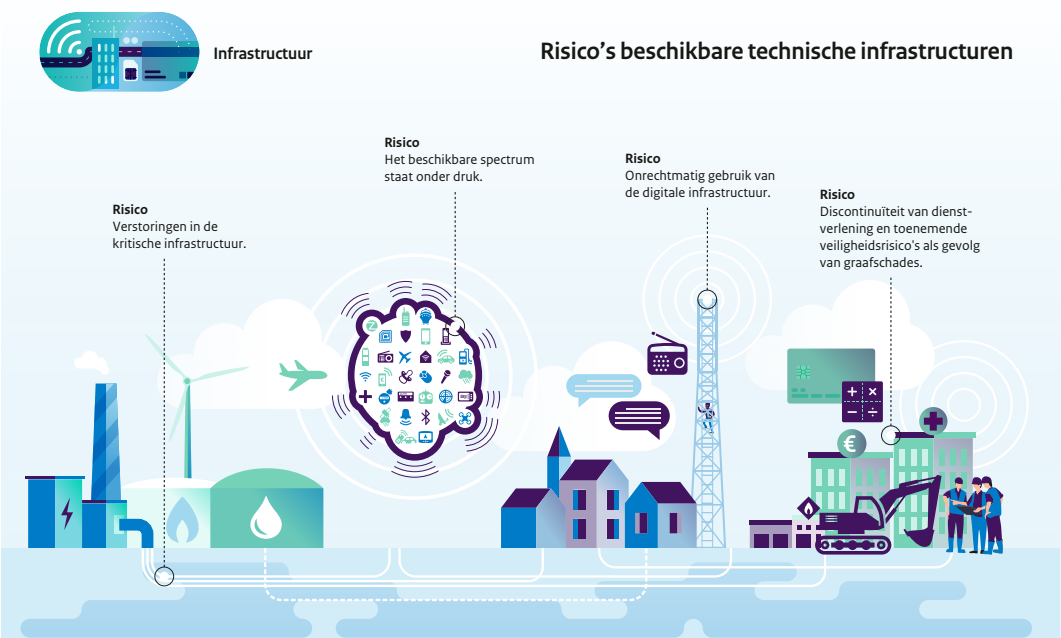
Is de infrastructuur aangelegd, verbonden en weerbaar?

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 bevorderen en beschermen wij de beschikbaarheid van draadloze en draadgebonden netwerken en de goede werking ervan. We streven naar een optimale beschikbaarheid, dekking en capaciteit van de (digitale) infrastructuur. Waarbij we storingsvrij gebruik kunnen maken van de netwerken en waar leveringszekerheid is met betrekking tot essentiële diensten.

Risico's



De geopolitieke situatie zal de komende jaren gespannen blijven. Vanuit de nationale en Europese veiligheid is er een toenemend belang om onderbrekingen van de kritische infrastructuur (zoals elektriciteit, gas, drinkwater en data) te voorkomen. Verder speelt voor de beschikbaarheid van een hoogwaardige digitale infrastructuur een verschuiving in het spectrum. Spectrumbanden die vroeger druk waren zijn nu rustiger, en met de ontwikkeling van de technologie zien we 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, maar ook door de in het kader van de energietransitie noodzakelijke verdichting en verzwaring van de energienetten ter voorkoming van congestie. Deze druk leidt tot grotere veiligheidsrisico's en meer discontinuïteit van dienstverlening vanwege graafschades.

Focuspunten

Toenemende drukte in specifieke delen van het frequentiespectrum

Het belang van veilig draadloos vitaal overheidsgebruik en de toenemende drukte in specifieke delen van het frequentiespectrum noopt tot de ontwikkeling en implementatie van innovatieve vormen van spectrumgebruik (gedeeld en dynamisch). Hierin werkt Nederland intensief samen met andere landen.

Dit doen we onder andere door uitvoering te geven aan de afspraken die gemaakt zijn op de World Radio Conference (WRC) 2023 en ter voorbereiding en uitvoering van afspraken tijdens de WRC 2027.

Van 5G naar 6G

Het 5G-netwerk is uitgerold en dit maakt allerlei nieuwe interacties en economische activiteiten mogelijk. De ontwikkelingen rondom 6G worden met onder meer onderzoeksinstituten en universiteiten verder verkend binnen het programma Future Network Services 6G, vanuit het Nationaal Groeifonds. Hierbij wordt bezien welke technologieën elkaar versterken in toekomstige situaties en welke risico's en scenario's ontstaan die van invloed zijn op de betrouwbaarheid van de digitale infrastructuur. Zie hiervoor ook Toekomstverkenning Digitale Economie 2030. Als RDI leveren wij kennis en expertise aan het programma Future Network Services.

Onrechtmatig gebruik van frequentieruimte

We constateren een toename in het onrechtmatig gebruik van het radiospectrum. In combinatie met de toenemende schaarste van frequenties bedreigt dit de beschikbaarheid van een hoogwaardige digitale infrastructuur. We moeten een toenemende inspanning plegen vanuit ons toezicht om deze onrechtmatigheid en daaruit volgende verstoringen tegen te gaan.

Voorkomen schade aan kabels in onze ondergrond

Er loopt een evaluatie van de 'Wet informatie-uitwisseling bovengrondse en ondergrondse netten en netwerken'. De uitkomst geeft de RDI naar verwachting effectievere mogelijkheden om met haar toezicht de risico's van graafschades te mitigeren. Het huidige uitgangspunt van de Wet (de graafketen lost het maatschappelijk probleem zelf op) is inmiddels verlaten. De nadruk ligt al enige tijd op verscherpt toezicht op de hele graafsector. Naast een versteviging van de personele inzet in de komende jaren blijft communicatie met de sector bijvoorbeeld door middel van voorlichtingscampagnes noodzakelijk om deze nieuwe rol effectief uit te kunnen voeren.

Resultaten

We zorgen ervoor dat Nederland ook in 2025 blijft beschikken over een hoogwaardige digitale infrastructuur middels benodigde frequentieruimte. We zorgen ervoor dat de beschikbare frequentieruimte is verdeeld naar gebruikers en gebruikstoepassingen en dat de verdeelde frequentierechten zijn beschermd en de aan gegunde rechten verbonden voorwaarden worden nageleefd. Het uitgangspunt hierbij is om de frequentieruimte op een dusdanige manier beschikbaar te stellen dat deze de meest (brede) waarde oplevert voor Nederland.

- In het komende jaar worden nieuwe afspraken over toegewezen frequentieruimte met andere ministeries gemaakt. Dit zijn de ministeries van: Defensie, Onderwijs, Cultuur en Wetenschap, Justitie en Veiligheid en het ministerie van Infrastructuur en Waterstaat.
- Ook wordt er een nieuwe uitgifte voorzien voor de Niet Landelijke Commerciële Omroepen.
- Daarnaast zorgen we ervoor dat de aanleg van kabels en leidingen in de Nederlandse ondergrond zo veilig mogelijk uitgevoerd wordt met zo min mogelijk impact op de beschikbaarheid van netwerken.

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

Samenleving vertrouwt op weerbare digitale infrastructuur

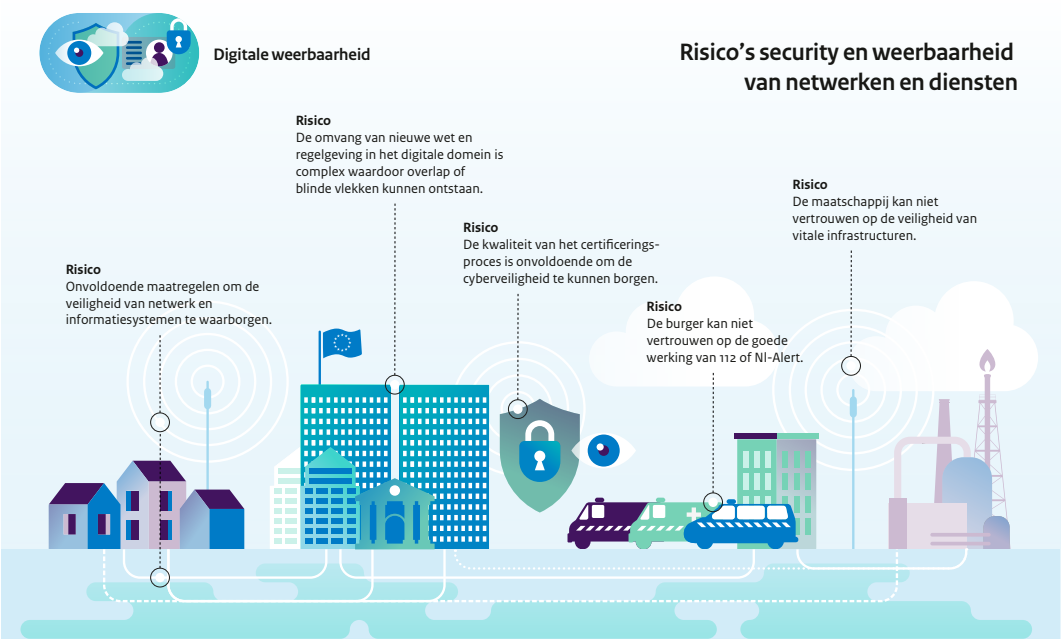
Maatschappelijke opgave

De Nederlandse samenleving rekent op de continuïteit, integriteit, vertrouwelijkheid en authenticiteit voor alle dienstverlening die gebruikmaakt van die digitale infrastructuur, zodat de economie en maatschappij daar ongestoord en in vertrouwen gebruik van kunnen maken.

Nederland speelt als digitaal knooppunt een belangrijke rol in de wereld. Weerbaarheid van die infrastructuur vraagt om zowel het nemen van verantwoordelijkheid door de aanbieders van de infrastructuur als een actief toezicht daarop. De digitale infrastructuur moet in dit opzicht breed gelezen worden en omvat bijvoorbeeld ook cloudaanbieders, datacenters en zeekabels. Wij zetten ons toezicht in om bij te dragen aan een veilige digitale economie.

Daarom zorgen wij voor een betrouwbaar stelsel van toelating van elektronische vertrouwensdiensten en houden wij toezicht op het Europese stelsel van certificering van cyberveilige producten, processen en diensten. We bewaken en stimuleren de digitale weerbaarheid van vitale en essentiële dienstverleners van infrastructuur in sectoren als telecom, internet en energie en informeren de maatschappij over het belang van de eigen digitale weerbaarheid ten aanzien van (rest)risico's.

Risico's



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 meer toenemend 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 we in op het toetsen van die inzet en stimuleren we het nemen van de passende maatregelen.

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.

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 (Europese) wet- en regelgeving

De regelgeving die de basis vormt voor onze maatschappelijke opgave is de afgelopen jaren aangepast en uitgebreid waardoor onze opdracht uitbreidt. Vanaf 2025 worden verschillende nieuwe wetten van kracht zoals de nieuwe netwerk- en informatiesystemen richtlijn (NIS2) en de Electronic Identification And Trust Services (eIDAS) 2.0 verordening. Daarnaast zijn er trajecten zoals de strategische heroriëntatie eInvoicing (Peppol) en ontwikkelingen rond nieuwe Cybersecurity Act (CSA) certificeringen die veel inzet vragen.

Nieuwe technologieën

Quantumtechnologie heeft onder andere impact op encryptie. Het biedt zowel kans op betere bescherming als het risico op misbruik van kwetsbaarheden. Eenzelfde redenering geldt voor AI-toepassingen. Beheren en beheersen van de nieuwe technologieën is zowel voor ondertoezichtgestelden als voor de RDI van groot belang.

Nieuwe manier van samenwerken

We delen onze kennis over digitale weerbaarheid en de bevindingen uit ons toezicht proactief met ondertoezichtgestelden en de samenleving. Zo werken wij mee aan meer bewustwording rond digitale weerbaarheid en beter beleid. Ook hebben we een actieve en coördinerende rol om samenwerking tussen diverse toezichthouders te versterken. Nieuwe wetgeving, maatschappelijke ontwikkelingen en streven naar efficiency en effectiviteit vragen daar om.

Resultaten

- We zijn benaderbaar en zoeken ondertoezichtgestelden in een vroeg stadium proactief op. We vertellen wie we zijn, wat we doen en wat we van ondertoezichtgestelden verwachten. We geven uitleg over (open) normen, zorgen voor voorspelbare processen en bieden guidance ('richtinggevend advies').
- We voeren inspecties uit om zo een beeld te vormen over de staat van de naleving. Dit beeld passen we toe om op organisatie, branche en sector acties in te zetten om de naleving van de wetgeving te stimuleren.
- We delen onze bevindingen proactief met de samenleving, beleidsmakers en de Europese Unie en zorgen voor doorontwikkeling van het Samenhangend Inspectiebeeld (SIB).
- We trekken nauw op met andere overheidsorganisaties die zich bezighouden met digitale weerbaarheid, zoals het Digital Trust Center en het Nationaal Cyber Security Centrum. We zorgen bijvoorbeeld voor een gezamenlijk vocabulaire en informatieproducten.
- We nemen het voortouw bij het uitbouwen van publiek-private netwerksamenwerking. We vertegenwoordigen bijvoorbeeld de toezichthouders in een werkgroep voor publiek-private samenwerking en voeren constructief overleg met brancheorganisaties.
- Door onze inzet op de toelating van vertrouwensdiensten en door het toezicht op het stelsel van certificering van cyberveilige producten, diensten en processen krijgt onze poortwachtersfunctie nadrukkelijker invulling.

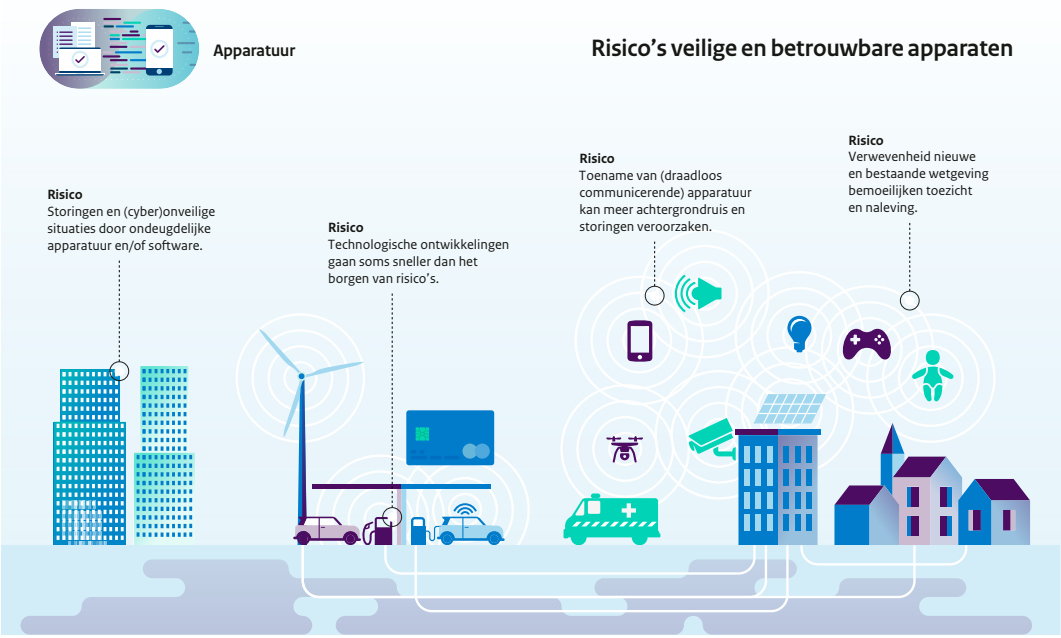
Werken de apparaten en instrumenten goed en veilig?

Apparaten nu en in de toekomst veilig en betrouwbaar

Maatschappelijke opgave

De Nederlandse samenleving rekent op veilige en betrouwbare apparaten binnen de digitale en analoge infrastructuur. Nederland kan erop vertrouwen dat apparatuur onder duidelijke randvoorwaarden en volgens geldende regelgeving in de handel is gebracht. En dat apparatuur (waaronder apparaten, software en installaties) storingsvrij en binnen toegewezen frequentieparameters werkt, elektrisch en elektromagnetisch veilig is, toegankelijk is, correcte hoeveelheidsinformatie bij handelstransacties weergeeft en cyberveilig is. Dit doen we onder andere door mee te werken bij het stellen van kaders die veilige en betrouwbare apparatuur waarborgen. Daarbij hebben we oog voor zowel de hardware als de software van het apparaat.

Risico's



Nieuw type normering en toezicht

Als gevolg van de digitalisering van de maatschappij en de steeds grotere maatschappelijke afhankelijkheid van digitale producten wordt de cyberveiligheid van apparatuur steeds belangrijker. Een digitaal apparaat dat vandaag cyberveilig is, kan morgen door een update of het ontbreken van een tijdige update, niet meer cyberveilig zijn. Om veiligheid en betrouwbaarheid van digitale producten te blijven borgen, is inzet op nieuw type normering en de wijze waarop we toezicht gaan houden van groot belang. Daarnaast is de veiligheid van digitale producten op de andere gebieden ook steeds meer afhankelijk van software-aansturing. Een integrale risicobeoordeling vanuit alle relevante veiligheidsaspecten is meer dan ooit noodzakelijk.

Verwevenheid disruptieve technologieën

Ontwikkelingen gaan sneller dan wet- en regelgeving. De gestage opkomst van quantumtechnologie en de ontwikkeling van AI zullen naar verwachting verstrekkende en op korte termijn gevolgen hebben. In toenemende mate komt apparatuur op de markt die zowel draadloos communiceren, digitale elementen bevatten, maar 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 apparatuur te blijven borgen is inzet op trends, integrale risicoanalyse, handelingsperspectieven en een netwerksamenwerking met opdrachtgever, andere relevante toezichthouders en stakeholders noodzakelijk.

Nieuwe maatschappelijke uitdagingen
Door toename van de hoeveelheid (draadloos communicerende) apparatuur voor diverse toepassingen, neemt ook de hoeveelheid (door apparatuur veroorzaakte) achtergrondruis en storingen toe. Eén apparaat kan voldoen aan de normen, maar bij grote aantallen apparatuur kan verstorende achtergrondruis (Man Made Noise) of een niet acceptabele grotere storing in het spectrum ontstaan, waardoor apparaten niet meer werken zoals verwacht. Dit effect wordt negatief versterkt door de toename van apparaten uit landen als China die veelal direct door consumenten worden geïmporteerd. Om veiligheid en betrouwbaarheid van apparatuur te blijven borgen, is inzet op het voorkomen van accumulatieve storing en inzet op het weren van ondeugdelijke importapparatuur noodzakelijk.

Verwevenheid nieuwe en bestaande wet- en regelgeving
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) hebben een steeds sterkere invloed op apparatuur die ook onder de Radioapparaten-richtlijn of EMC-richtlijn valt. Om veiligheid en betrouwbaarheid van apparatuur te blijven borgen is het noodzakelijk om met een brede integrale blik naar nieuwe en bestaande wetgeving te kijken, door middel van netwerksamenwerking en informatie-uitwisseling met andere relevante toezichthouders.

Focuspunten

Nieuw type normering en toezicht
Inzet op standaardisatie en toezicht onder Radio Equipment Directive (RED) 3.3 d.e.f., Cyber Resilience Act (CRA) en AI vraagt om een nieuw type normering en een meer integrale risicobeoordeling vanuit het toezicht.

Verwevenheid disruptieve technologieën
Meer focus op trends, integrale risicoanalyse, handelingsperspectieven en een netwerksamenwerking met opdrachtgever, andere relevante toezichthouders en stakeholders op thema's als energietransitie, AI, Quantum en digitale product vraagstukken.

Nieuwe maatschappelijke uitdagingen
Inzet op Man Made Noise en het voorkomen van accumulatieve storing. Dit vraagt meer van de RDI op het gebied van monitoren en optreden tegen onwenselijke situaties. Het weren van ondeugdelijke importapparatuur vraagt naast een verhoogde toezichtinspanning aanvullende beleidsinstrumenten om de aanvoer te stoppen.

Verwevenheid nieuwe en bestaande wet- en regelgeving
Verdere ontwikkeling van een brede integrale blik op nieuwe en bestaande wetgeving, middels uitbreiden van inzet op wetgevingsondersteuning, standaardisatie en netwerksamenwerking en informatie-uitwisseling met andere relevante toezichthouders.

Resultaten

- Eisen aan apparatuur zijn zoveel mogelijk gestandaardiseerd en genormaliseerd.
- Nederland beschikt over de benodigde internationale frequentieruimte en gestandaardiseerde eisen voor apparatuur gebruik.
- Nederland beschikt over een actueel Nationaal Frequentieplan, zodat stakeholders zekerheid hebben over de frequentiebestemmingen en (apparatuur-)eisen vanuit spectrumengineering .
- Storingen op frequentiegebruik door apparatuur worden vroegtijdig onderzocht en daar waar mogelijk weggenomen.

- Relevante wet- en regelgeving (conformiteitsregels) ten aanzien van apparatuur wordt bewaakt en gehandhaafd.
- De (inter)nationale regelgeving en de bijbehorende guidance op metrologie passen we aan met name in relatie tot de ontwikkelingen ten gevolge van de energietransitie, zoals rond laadpalen en waterstof.
- 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 wordt het kerndepartement geadviseerd over nieuwe of bestaande wet- en regelgeving.

Hierbij staat het systeem centraal en kijken wij integraal naar het geheel van kaderstelling, toelating en ordening, bewaken en onderzoeken.

Onder de aandacht: Moderne wetgeving en weerbare infrastructuur voor Caribisch Nederland

Maatschappelijke opgave

De digitale transitie voor Caribisch Nederland vraagt van ons dat we 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, St. Eustatius en Saba) en onderliggende regelgeving en zorgen wij voor een veilig verbonden Caribisch Nederland.

Risico's

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. Deze omstandigheden hebben invloed op en zorgen voor uitdagingen ten aanzien van de onderwerpen beschikbaarheid (waaronder continuïteit), authenticiteit, vertrouwelijkheid en integriteit. Maatschappelijk gezien worden deze onderwerpen steeds belangrijker omdat de burgers en bedrijven in Caribisch Nederland volwaardig mee moeten kunnen doen aan de digitale economie. Daarvoor is nodig dat een aantal basisvoorzieningen op orde zijn en blijven, waaronder een stabiele en duurzame digitale infrastructuur.

Focuspunten

Inzet op digitale weerbaarheid

Door bovengenoemde risico's is het toezicht op deze onderwerpen een nadrukkelijker thema. De RDI handelt daarbij niet alleen vanuit een wettelijke taak, maar ook vanuit haar maatschappelijke verantwoordelijkheid. Daarnaast geeft de RDI nadere invulling aan het toezicht op de normen die er zijn ten aanzien van beschikbaarheid (waaronder continuïteit), authenticiteit, vertrouwelijkheid en integriteit door onder meer het opstellen van toezichtarrangementen waarbij de telecomaanbieders betrokken worden. Samen met onze collega's van onze Directie Digitale Weerbaarheid, de directie Digitale Economie van het Ministerie van Economische Zaken, Digital Trust Center (DTC), Nationaal Cyber Security Centrum (NCSC) en de Kamers van Koophandel in Caribisch Nederland willen we werken aan bewustwording op het gebied van cyberveiligheid.

Samenwerken aan nieuwe wetgeving

Wij werken samen met de directie Digitale Economie van het Ministerie van Economische Zaken en de Autoriteit Consument & Markt (ACM) aan nieuwe telecomwetgeving die beter past bij de huidige situatie. Het is hierbij belangrijk dat we aandacht hebben voor de lokale situatie, de kleinschaligheid en differentiatie van de eilanden in Caribisch Nederland. Naar verwachting brengt dit meer taken en bevoegdheden met zich mee voor het team Caribisch Nederland. Voor alle nieuwe wetgeving geldt dat er voor de BES-eilanden het principe 'comply or explain' moet worden toegepast.

Versterken van de uitvoeringskracht

Voor Caribisch Nederland is het extra belangrijk om de samenwerking te zoeken, omdat kennis, expertise en middelen schaarser zijn dan in Europees Nederland. De RDI werkt al nauw samen met een aantal overheidsorganisaties, zoals de ACM, de Rijksdienst Caribisch Nederland, de Regulatory Authority of Curaçao en het Bureau Telecommunicatie & Post in Sint Maarten. Door samenwerking wordt op een effectievere en efficiëntere manier toezicht gehouden. Daarom wordt de samenwerking gezocht met andere overheidsorganisaties die zich bezig houden met dezelfde maatschappelijke vraagstukken als de RDI. Denk aan: de Douane, Kustwacht, Scheepvaartinspectie, Commissariaat voor de Media en de Openbare Lichamen.

Resultaten

De komende jaren zet de RDI meer in op de digitale weerbaarheid van Caribisch Nederland. Samen met de concessiehouders wordt invulling gegeven aan open normen, zoals het waarborgen van continuïteit en integriteit van netwerken en wordt hier toezicht op gehouden. Daarnaast wordt ingezet op bewustwording, ook op onderwerpen waar (nog) geen taak ligt voor de RDI, maar wel een maatschappelijke verantwoordelijkheid wordt gevoeld. Het resultaat hiervan is dat de concessiehouders stap voor stap passende en organisatorische maatregelen nemen, waardoor risico's voor zowel de concessiehouders, als de consument en de maatschappij in zijn geheel worden verkleind.

Samen met de directie Digitale Economie en ACM werken we toe naar wet- en regelgeving die past bij de lokale situatie, maar ook bij de huidige stand van de techniek. Dat betekent dat de komende jaren een moderniseringsslag plaatsvindt in de huidige wet- en regelgeving. Daarnaast vindt een moderniseringsslag plaats in de door de RDI uitgegeven concessies en machtigingen.

De RDI werkt al met een aantal organisaties samen aan gezamenlijke onderwerpen. Dit moet de komende jaren resulteren in duurzame samenwerkingsverbanden. Deze samenwerkingsverbanden bevorderen een effectieve en efficiënte manier van toezichthouden, zowel voor de verschillende diensten als voor de maatschappij.

De RDI als organisatie in beeld

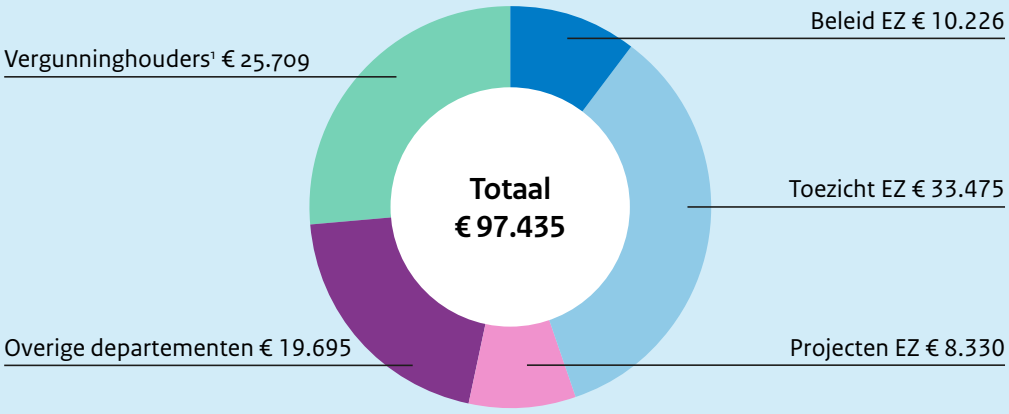
Organisatiecijfers

De RDI valt als rijksinspectie en publieke dienstverlener onder de verantwoordelijkheid van de minister van Economische Zaken. Met onze vier kernactiviteiten voorkomen we in de kern risico's voor de samenleving, zoals deze zijn weergegeven in de vorige hoofdstukken. We kijken waar zaken verbeterd kunnen worden en spreken daarover met belanghebbenden en vertegenwoordigers van de samenleving.

Onze begroting voor 2025

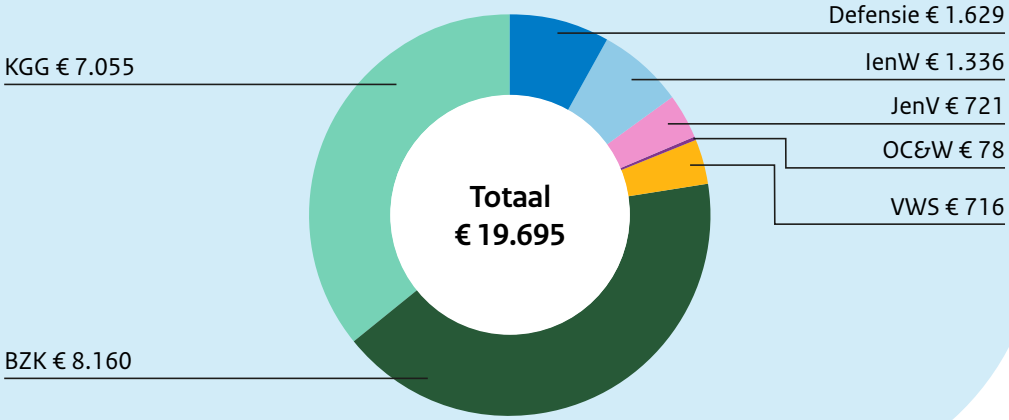
Financiële cijfers RDI 2025

Bedragen x 1.000



Financiële cijfers overige departementen[2]

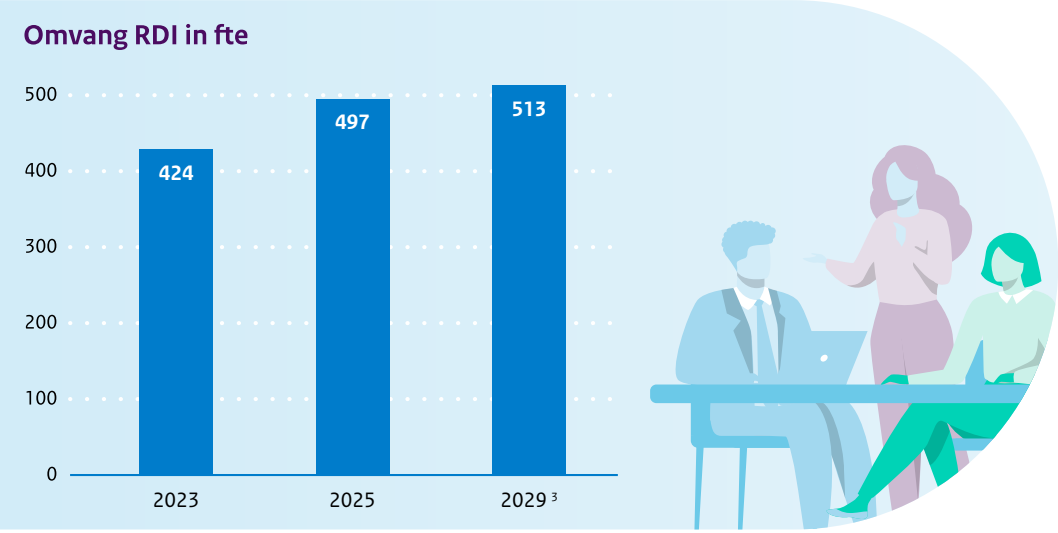
Bedragen x 1.000



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

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

Groei RDI in FTE's



3: Verwachte groei van het personeelsbestand als gevolg van de groeiende opdracht op de herziening van de Netwerk- en informatiesystemen (NIS2) en de Europese richtlijn voor Critical Entities Resilience (CER).

Continuïteit RDI

Continuïteit van onze dienstverlening is essentieel om onze maatschappelijke opgaven nu, maar ook in de toekomst, te borgen. De RDI is naast de inhoudelijke maatschappelijke opgaves gericht op het optimaal uitrusten van de mensen en middelen ten behoeve van die opgaves. De kwaliteit van ons werk betreft enerzijds de vraag of we de goede dingen doen en anderzijds of we de dingen goed doen. Daarvoor is het nodig dat onze processen, producten en strategie kwalitatief en goed geborgd zijn. Daarnaast werkt de RDI continu aan strategische personeelsplanning (SPP) om te weten waar behoefte aan is in het licht van nieuwe opdrachten en/of (ver)nieuw(d)e werkwijzen.

De RDI versterkt de informatiepositie en sturing van de gehele organisatie en draagt zorg voor een professionele dienstverlening. Voor de RDI is het belangrijk om de komende jaren de eigen informatiehuishouding verder te professionaliseren om optimaal transparant en open te kunnen zijn en de dienstverlening, waaronder de digitale dienstverlening, te kunnen versterken en versnellen. De RDI streeft daarom naar data en informatie die volledig, betrouwbaar, vindbaar en duurzaam toegankelijk is voor burger, ondernemer en maatschappij.

De RDI kan zo steeds mee bewegen met de veranderende maatschappelijk vraag. Daarmee houden we Nederland veilig verbonden.

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 2024

#wijzijnRDI