Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Staan voor een veilige en weerbare digitale infrastructuur

Jaarplan 2023
Rijksinspectie Digitale Infrastructuur

Voorwoord

Veiligheid in vooruitgang
Met het kompas gericht op digitalisering, zet Nederland voortvarend koers naar morgen. Digitalisering is de kortste route naar een duurzame, veilige en veerkrachtige samenleving. En in veel gevallen het antwoord op de complexe maatschappelijke vragen die op ons afkomen. De Nederlandse ambities op het gebied van digitalisering zijn dan ook groot: Nederland wil de digitale koploper van Europa worden. En is daarbij goed onderweg: ons land behoort tot de best presterende digitale economieën van Europa. Met volop mogelijkheden om de kansen van digitalisering te verzilveren! Dat is geen vanzelfsprekendheid. Want hoewel kansrijk, is digitalisering ook kwetsbaar. De digitale infrastructuur staat onder druk. En die dreiging is permanent en neemt zelfs toe, zo blijkt uit de Nederlandse Cybersecuritystrategie 2022-2028.

Geopolitieke verhouding verschuiven en verscherpen. En de digitale infrastructuur blijkt bij conflicten steeds vaker doelwit. Er rijzen vragen over privacy, ethiek en ecologie. En er zijn zorgen over de veiligheid van data, publieke waarden en onszelf. Er is meer actie nodig om de diverse verschijningsvormen van die dreiging het hoofd te bieden. Dat besef is groeiende. Ik zie een *prioriteiten-shift* ontstaan. Een sterkere focus op veiligheid, continuïteit en betrouwbaarheid. En meer aandacht voor het behoud van het vertrouwen dat zo voorwaardelijk is voor het verdere verloop van de digitale transitie die we doormaken.

Vanuit dat gegeven en vanuit die context maakte mijn organisatie vorig jaar de stap van Agentschap naar Rijksinspectie en van Telecom naar Digitale Infrastructuur. Vanaf 2023 heten wij *Rijksinspectie Digitale Infrastructuur.* Een naam die goed past bij onze huidige taken en verantwoordelijkheid. En ruimte biedt voor onze ambities. Als RDI zullen we nog beter in staat zijn aan te sluiten bij de opgaven waar Nederland zich voor gesteld ziet.

Met de aandacht die onze bestaande werkzaamheden en verantwoordelijkheden verdienen. En maximale focus op de toezichtstaken die de digitale veiligheid van Nederland vergt. Daarbij is het van het allergrootste belang te kunnen werken vanuit een onafhankelijke positie. Waarbij een wettelijke borging voldoende bandbreedte biedt om die keuzes te maken en die adviezen te formuleren die nodig zijn om Nederland digitaal weerbaar te houden. Onafhankelijk en onpartijdig toezicht is onmisbaar voor een goed openbaar bestuur. En om Nederland veilig verbonden te houden.

Angeline van Dijk
Mr. A.T.A.J. (Angeline) van Dijk
Inspecteur-generaal
Rijksinspectie Digitale Infrastructuur

Inhoudsopgave

1

Rijksinspectie Digitale Infrastructuur (RDI)

Digitalisering heeft Nederland ingrijpend veranderd in de manier waarop wij communiceren en toegang hebben tot diensten en informatie. Hier ligt een infrastructuur aan ten grondslag, die in toenemende mate digitaal is. Deze digitale infrastructuur is ons werkveld. Wij zorgen ervoor dat de digitale infrastructuur beschikbaar, betrouwbaar en veilig te gebruiken is.
Tegelijkertijd verandert de wereld snel en is er een toenemende behoefte aan veiligheid, die mede wordt ingegeven door geopolitieke ontwikkelingen. Cyberveiligheid, kunstmatige intelligentie, veilige apparatuur en de energietransitie zijn daarmee de issues van vandaag en morgen. Binnen ons brede werkveld die vele sectoren raakt, focussen wij ons op deze thema's.

1.1 De digitale infrastructuur als fundament

De digitale infrastructuur is het digitale fundament van onze moderne samenleving. Dit fundament is van wezenlijk belang voor ons dagelijks én ons toekomstig functioneren. De Rijksinspectie Digitale Infrastructuur is in staat om ónder de motorkap van de digitale infrastructuur te kijken. De digitale infrastructuur blijft voor velen namelijk onzichtbaar. Het is ons doel om dit fundament veilig en bruikbaar te maken en te houden. Met het kijken onder de motorkap bedoelen we dat we de technische kennis en expertise hebben om bijvoorbeeld de security en weerbaarheid goed te kunnen beoordelen, ten behoeve van ons toezicht op informatienetwerken, inclusief de onderliggende fysieke, analoge basisinfrastructuur. Maar ook ons werk ten aanzien van de cyberweerbaarheid van partijen in de IT- en energiesector, en onze werkzaamheden ten aanzien van de integrale veiligheid en bruikbaarheid van apparaten. Dit toezicht vindt voornamelijk op stelselniveau[1] plaats. Daarnaast houden we ons bezig met meer sectoraal toezicht binnen het digitale fundament, onder andere in de metrologie en het gebruik van identificatiemiddelen.

We zoeken actief de professionele samenwerking op met andere rijks- en markttoezichthouders en collega-overheidsorganisaties en onderhouden we actieve contacten met externe (branche en belangen-) organisaties. Tevens nemen we deel aan belangrijke internationale overleggen, zoals binnen het verband van de EU. Zo zorgen wij zo effectief en efficiënt mogelijk voor een veilig en verbonden Nederland.

1 Met stelseltoezicht bedoelen wij dat ons toezicht op de naleving, kwaliteit of veiligheid zicht uitstrekt over het gehele werkterrein, zodat informatie wordt verkregen over, sturing wordt gegeven aan, en verantwoording wordt afgelegd over het functioneren van het stelsel (of systeem) als geheel. (en daarmee niet slechts met betrekking tot specifieke individuele bedrijven of instellingen alleen).

1.2 Voor een veilig verbonden Nederland

Digitalisering is in toenemende mate verweven geraakt met bijna alle aspecten van ons dagelijks leven. Het biedt grote kansen voor de maatschappij en economie. We zien een diepgaande maatschappelijke afhankelijkheid van digitalisering en tegelijkertijd een toename van dreigingen en potentiële verstoringen. De samenleving moet er op kunnen vertrouwen dat wij maatschappelijke vraagstukken rond de digitale infrastructuur tijdig detecteren, risico's signaleren en belangen beschermen.

Ons doel is dan ook dat Nederland kan vertrouwen op de ***beschikbaarheid*** van de digitale infrastructuur, die ***continu*** en ***veilig*** te gebruiken is. Daarom richten wij ons op de volgende 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 vraagstukken van de digitale infrastructuur betreffen dus zowel de **beschikbaarheid** van de benodigde infrastructuur, de **betrouwbaarheid** hiervan, alsmede het **vertrouwen** in het gebruik ervan.

1.3 De RDI in drie thema's

Onze inzet ten aanzien van de digitale infrastructuur hebben we rondom drie thema's georganiseerd. Vanuit drie thematische directies werken we als RDI multidisciplinair samen aan onze maatschappelijke opgave; een veilig verbonden Nederland.

Directie Infrastructuur: Beschikbare technische infrastructuren

De Nederlandse samenleving rekent op een hoogwaardige analoge[2] en digitale infrastructuur. De RDI bevordert en beschermt de **beschikbaarheid** van draadloze en draad-gebonden netwerken, net zoals de **dekking** en **capaciteit** van de infrastructuur en een **goede**, **storingsvrije werking** hiervan. Dit doen we onder andere door het **frequentiespectrum** in internationaal en nationaal verband te verdelen en de gebruiksrechten op dat spectrum toe te kennen en, waar dat vanuit onze toezichtstaak noodzakelijk blijkt, in te trekken.

2 Bij analoge technologie blijft het oorspronkelijke signaal in tact, terwijl bij digitale technologie het signaal wordt omgezet in bits.

Directie Digitale weerbaarheid: Security en weerbaarheid van netwerken en diensten

Daarbij dragen wij zorg voor de **continuïteit**, **integriteit**, **vertrouwelijkheid** en **authenticiteit** van de digitale infrastructuur, zodat consumenten en ondernemers, die hun diensten over 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 **electronic identification en authenticatie** bij toegang tot de overheid. 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.

Directie Apparatuur: Veilige en betrouwbare apparaten

Daarnaast zetten wij ons in voor veilige en betrouwbare apparaten. Nederland kan er op vertrouwen dat apparatuur onder duidelijke randvoorwaarden en volgens geldende regelgeving in de handel is gebracht. En dat apparatuur storingsvrij werkt, **elektrisch en elektromagnetisch veilig** 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.

Lees meer over onze programmering in hoofdstuk 3.

1.4 Onze kernwaarden

We reflecteren regelmatig op wat we doen in lijn is met onze opgave, rol en taak binnen de digitale infrastructuur. Vanuit een **gedeelde visie** en een **maatschappelijke verantwoordelijkheid** werken we bij RDI aan een veilig verbonden Nederland. We voorzien vanuit onze **professionaliteit** ontwikkelingen en trends, en geven daar een constructieve invulling aan. We schromen niet om het voortouw te nemen, knelpunten te signaleren of gevoelige dossiers op te pakken. En door **samenwerking** te zoeken met de markt, experts, beleidsmakers, zowel nationaal als internationaal, zorgen we er met onze partners voor dat de digitale infrastructuur, ondanks de snelle ontwikkelingen, voor iedereen beschikbaar en betrouwbaar blijft. Een digitaal netwerk waar Nederland altijd op kan vertrouwen.

2

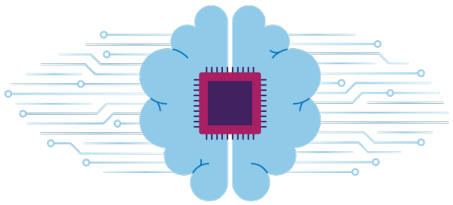
Impact van ontwikkelingen in de digitale infrastructuur

De RDI geeft in haar taken uitvoering aan de wetgeving, binnen de kaders die vanuit nationale en Europese wet- en regelgeving op de digitale infrastructuur afkomen. Daarnaast sluiten we aan bij nationale (beleids) kaders, zoals de Strategie Digitale Economie en Nationale Cybersecuritystrategie. Maar onze opdracht is breder, gericht op de publieke belangen in de digitale infrastructuur. We brengen daarom de mogelijke impact van toekomstige ontwikkelingen vroegtijdig in kaart.

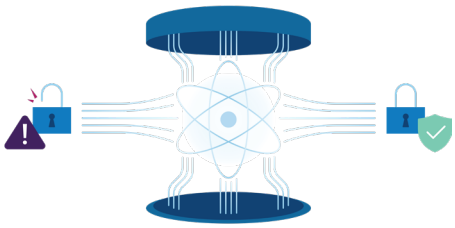
In dit hoofdstuk schetsen we een aantal belangrijke ontwikkelingen in de digitale infrastructuur dat van invloed is op onze rol en taken. Deze ontwikkelingen kunnen we onderverdelen in twee overkoepelende trends: 1) impactvolle technologische trends en 2) de toename van digitale regulering vanuit Europa. Vervolgens gaan we in op de gevolgen van deze ontwikkelingen op de positie van de RDI en de thema-overstijgende speerpunten waarop zij zich inzet.

2.1 Impactvolle technologische trends

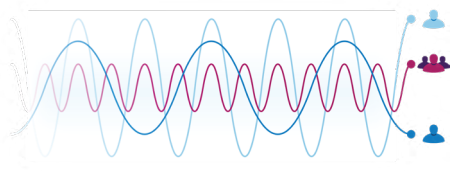
We zien de impact van technologische trends en ontwikkelingen op het werkveld van de digitale infrastructuur toenemen. Denk hierbij aan de explosieve ontwikkeling van Artificiële Intelligentie (AI), kwantumtechnologie, toekomstige netwerk- en informatiesystemen (5G en 6G) en de maatschappelijke en economische vervlechting van digitale ecosystemen.



Dilemma's door groei AI en algoritmes



Toename kwetsbaarheid van versleutelde informatie door kwantumtechnologie



Innovatie voor dynamisch spectrumgebruik belangrijker

Future networks en 6G leiden tot vervlechting digitale ecosystemen en netwerken

Onze digitale infrastructuur is de basis geworden voor duurzame economische groei. We spreken daarom van een digitaal ecosysteem: een netwerk van stakeholders, partners en actoren, die actief zijn in allerlei vormen, sectoren en rollen. Complexe integratie van digitale systemen, processen en leveranciers met dynamische producten en diensten, waarvan we als samenleving afhankelijk zijn, kenmerken het systeem.

Technologische trends, zoals **Artificial Intelligence** (AI) en **kwantumtechnologie**, raken de digitale infrastructuur daardoor in de breedte. Door de centrale positie in onze samenleving is de infrastructuur in toenemende mate verweven met belangrijke sectoren, zoals financiën, zorg, transport, en energie. Denk hierbij aan energiemeters, zonnepanelen en laadpalen die onderling gekoppeld zijn in het slim gestuurde energienetwerk, of denk aan de sensoren en robots in een productieproces. Veel apparaten vormen een schakel in een groter digitaal proces of systeem.
Deze en andere trends bieden kansen, maar kunnen ook bedreigend zijn voor de beschikbaarheid, integriteit en betrouwbaarheid van de digitale infrastructuur.

Overkoepelende maatschappelijke thema's als **economische groei, gezondheid, duurzaamheid, klimaat, mobiliteit en veiligheid** komen bij elkaar. We zien dat een integrale blik essentieel is om te begrijpen hoe verschillende technologische en maatschappelijke ontwikkelingen ingrijpen op de alsmaar complexer wordende infrastructuur. Eveneens gecompliceerd door diverse en soms tegengestelde belangen van stakeholders in de digitale infrastructuur. Dit vraagt van ons een anticiperende en onderzoekende opstelling in het werk van de RDI ten aanzien van het gehele systeem waarop zij toezicht houdt. **De RDI onderzoekt daarom in 2023 kansen en risico's van impactvolle technologische ontwikkelingen als AI en kwantumtechnologie.**

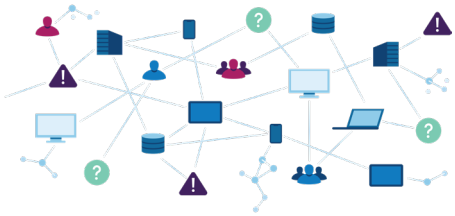
AI

Het gebruik van moderne AI-algoritmes maakt het mogelijk om complexe digitale processen, robots en netwerken te automatiseren en te sturen. Dat brengt nieuwe maatschappelijke, ethische en veiligheidsvraagstukken met zich mee, bijvoorbeeld ten aanzien van de controle op algoritmes. Het Europese debat loopt en de regelgeving voor AI is in ontwikkeling. De verwachting is dat er toezicht gehouden gaat worden op het gebruik van algoritmes in toepassingen.

Kwantumtechnologie

Dankzij kwantumtechnologie kunnen in de toekomst een groot aantal berekeningen tegelijkertijd uitgevoerd worden. Hierdoor kan de huidige encryptie makkelijker gekraakt worden. Aangezien encryptie een belangrijke manier is om netwerken en informatiesystemen te beveiligen, ontstaan risico's voor de digitale samenleving.

Toename geopolitisering van de digitale infrastructuur



Toename complexiteit van digitale ecosystemen

Groei regelgeving ten behoeve van digitale soevereiniteit

Sterke toename regelgeving digitale infrastructuur

2.2 Toename digitale regulering vanuit Europa

De RDI zal de komende jaren geconfronteerd worden met een omvangrijk pakket aan digitale regulering dat de Europese Commissie inzet in de Europese digital age. Deze regelgeving ziet onder meer toe op vraagstukken van **veiligheid en continuïteit van de digitale infrastructuur en het gebruik van data en persoonsgegevens**. Deze regels brengen nieuwe organisatorische en coördinerende uitdagingen mee ten aanzien van samenwerkend toezicht en aanliggende verantwoordelijkheden. Wij zijn hierover voortdurend in gesprek met collega toezichthouders en stakeholders.

Binnen Nederland en Europa neemt het besef toe dat afhankelijkheid van marktspelers ook risico's meebrengen, bijvoorbeeld als het gaat om het houden van regie en controle over de digitale infrastructuur, dat wil zeggen; de digitale autonomie. De wereldpolitiek raakt daardoor betrokken en stuurt sterker op de randvoorwaarden die hieraan gekoppeld zijn. De Europese Commissie lanceert in opvolgende stappen regelgeving waarmee zij stuurt op de ontwikkeling van de digitale markt in Europa.

Als toezichthouder en uitvoerder krijgt de RDI de komende jaren te maken met de impact van een groeiend aantal nieuwe wet- en regelgeving.

2.3 De positie van de RDI verandert

Digitale technologie verandert het leven van mensen. De digitale strategie van de EU is erop gericht de digitale transformatie te laten werken voor mensen en bedrijven. De Europese Commissie is vastbesloten om deze periode het "**digitale decennium**" van Europa te maken[3]. Er is sprake van een versterking van digitale autonomie en het zelf vaststellen van normen en kaders, - in plaats van die van anderen te volgen – met een duidelijke focus op data, technologie en infrastructuur. De uitwerking hiervan is te zien in de wijze waarop het nationale toezicht en de uitvoering van nieuwe kaders voor de digitale samenleving vorm krijgen.

Horizontale (generieke) kaders zoals de **Cybersecurity Act** (**CSA**) en de **Cyber Resilience Act** (**CRA**) hebben effect op meerdere beleidssectoren. Ook kaders voor netwerken en energie, zoals de richtlijn **Network and Information Security 2** (**NIS2**), hebben door de centrale positie in de samenleving overlap in de digitale eisen voor de markt. We voeren in 2023 onze taken conform de wet- en regelgeving uit en hebben daarbij tevens oog voor het maatschappelijke doel waarvoor ze dienen. Wat dit specifiek voor activiteiten en stakeholders betekent is te vinden in hoofdstuk 3.

De RDI zet in op **multidisciplinaire samenwerking** met andere toezichthouders of beleidsdepartementen. Bovendien krijgt de RDI, naast het Ministerie van Economische Zaken en Klimaat, meer taken vanuit andere ministeries, zoals het Ministerie van Justitie en Veiligheid en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Ook wordt de RDI vaker gevraagd om mee te denken met sectorale toezichthouders.

Al deze ontwikkelingen overstijgend, zien we dat de rol en positie van de RDI in het digitale ecosysteem verbreedt **van een sectorale toezichthouder, naar een meer horizontale en generieke toezichthouder**. Gezien de vele knooppunten en overlappende inhoud, acht de RDI cross-sectorale dan wel horizontale samenwerking cruciaal. Omdat het stelsel nog volop in ontwikkeling is, gaat de RDI de komende jaren het totaalpakket aan nieuwe regelgeving voor de digitale infrastructuur in kaart brengen en verkennen wat de horizontale positie van de RDI kan betekenen voor het totale stelsel en daarmee de samenleving. We blijven reflecteren op de eigen positie in de diverse netwerken, we actualiseren risicoanalyses en starten nieuwe samenwerkingsvormen vanuit een breed en integraal perspectief.

[3] Europa's digitale decennium: doelstellingen voor 2030

3

Onze focus in 2023

De drie directies binnen onze organisatie dragen met thema specifieke prioriteiten bij aan de realisatie van een veilig en verbonden Nederland. In lijn met de trends en ontwikkelingen uit het vorige hoofdstuk en op basis van een risico-inschatting zet de RDI voor 2023 in op de onderstaande speerpunten. Dit doen we voornamelijk op **stelselniveau**. Vanuit onze hoofdthema's houden we zicht op het functioneren, de bedreigingen en de risico's op de (digitale) infrastructuur, netwerken en diensten en de hedendaagse (slimme) apparatuur.
Hier houden we toezicht op. Daarnaast staan we klaar voor ondersteuning en advies, signaleren en agenderen we bedreigingen. Daarbij zetten we ons in om de digitale infrastructuur breed in de maatschappij te versterken. Vanuit deze opgave richten we ons daarbij op de vraagstukken:

Is de infrastructuur aangelegd, verbonden en weerbaar?
- Ben ik bereikbaar op mijn mobiel en kan ik zelf bellen vanuit dit natuurgebied of drukbezocht festivalterrein?
- En hoe zit dat met het bellen van het alarmnummer 112?
- Kan ik met 5G op mijn mobiel werken in de trein?
- Blijft de kabel naar mijn laadpaal ongeschonden bij graafwerkzaamheden?
- Heb ik mijn antenne-opstelpunt voldoende beveiligd tegen brand of vernieling?
- Kan ik als lokale omroep straks uitzenden op DAB+?

Zijn de netwerken en diensten continu bereikbaar, integer en veilig?
- Hartbewaking op afstand; is dat wel veilig?
- Kan ik mijn digitale handtekening veilig en betrouwbaar gebruiken?
- Kunnen klanten bij een aankoop via mijn bedrijfswebsite veilig een financiële transactie doen?
- Heb ik nog elektriciteit in geval van een hack bij mijn netbeheerder?
- Hoe kan ik als ondernemer er voor zorgen dat mijn kassasysteem blijft functioneren?

Werken de apparaten en instrumenten goed en veilig?
- Kan iemand mij afluisteren via de babyfoon?
- Verstoort de omvormer in mijn zonnepanelen mijn WIFI ontvangst in huis niet?
- Bied ik cyberveilige "slimme" apparatuur aan op mijn website?
- Is de elektromagnetische straling van de antenne op mijn flatgebouw onder de limiet?
- Is de 50 liter benzine die ik net tankte ook echt 50 liter?

3.1 Beschikbare technische infrastructuren

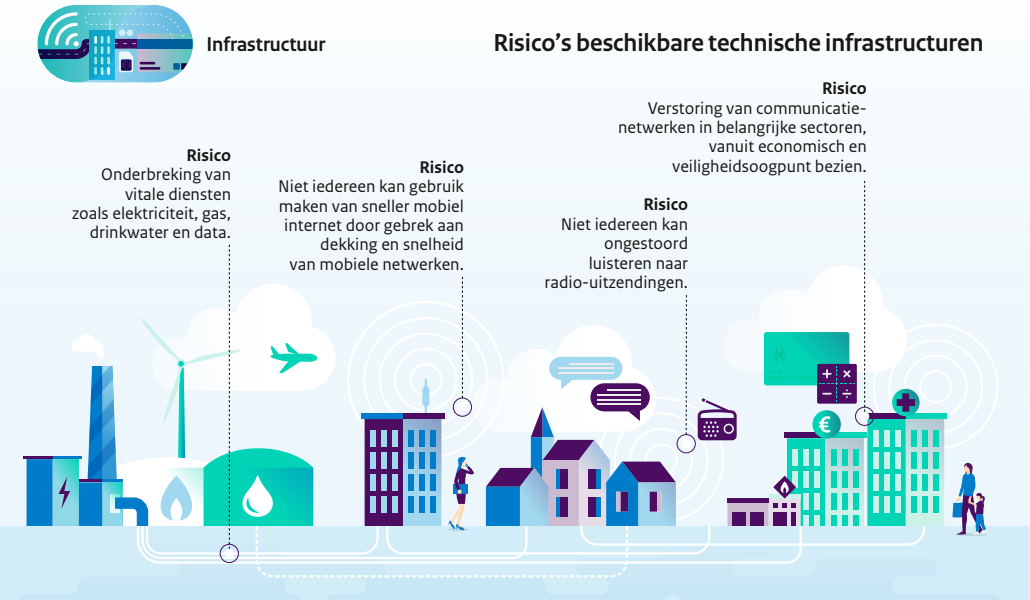
Maatschappelijk belang: Is de infrastructuur aangelegd en verbonden?

Onze activiteiten binnen het domein van de technische infrastructuren richten zich op de beschikbaarheid en het storingsvrij gebruik van netwerken waar de lucht- en scheepvaartsector, de OOV[4]-diensten, bedrijfsnetwerken, satellietnetwerken en de openbare telecom- en omroepnetwerken gebruik van maken.

Voor hun maatschappelijke en economische belangen moeten burgers en bedrijven kunnen vertrouwen op de aanwezigheid en goede werking van de (digitale) technische infrastructuur.

[4] Diensten die vallen onder de Openbare Orde en Veiligheid.

Hierbij is een aantal risico's te onderkennen die we mede door onze inzet in 2023 willen mitigeren. Zie hiervoor onderstaande figuur.



De focus van onze inspanningen leggen we in 2023 op:

1 Nederlandse inbreng World Radio Conference: WRC23

In 2023 wordt de World Radio Conference 2023 (WRC23) in Dubai gehouden. Hier vinden mondiale onderhandelingen over de verdeling van het spectrum plaats. Door onze inzet van expertise en technische kennis, werken we mee aan de **behartiging van de Nederlandse belangen** en zetten we in op een **toekomstige beschikbaarheid van frequentieruimte** die optimaal de Nederlandse en Europese belangen dient.

2 Verdeling schaarse frequenties via veilingen

De beschikbaarheid van digitale infrastructuur vergt een verdeling van het schaarse frequentiespectrum. We kunnen het spectrum op deze manier doelmatig benutten voor toepassingen waaraan maatschappij en economie waarde toekent, zoals mobiele communicatie en omroep. Het jaar 2023 staat in het teken van twee grote verdelingen op basis van een veiling; de veiling van de **3,5 GHz band** ten behoeve van **mobiele communicatietoepassingen** en de veiling van de frequentiekavels ten behoeve van **commerciële radio** (zowel analoog/FM als digitaal/DAB+).

Voordat we de frequentieruimte in de 3,5 GHz-band kunnen verdelen, dienen we bestaand lokaal gebruik in deze band te migreren. In 2023 is de inzet gericht op het realiseren van deze migratie, door middel van het opstellen en uitvoeren van een migratieplan, monitoring van de uitvoering van dat plan door vergunninghouders, en het detecteren en eventueel interveniëren bij synchronisatieproblemen tussen lokaal gebruik onderling en/of met het landelijk openbaar gebruik.

3 Klaar voor de toekomst: dynamisch spectrummanagement

De toenemende schaarste aan het frequentiespectrum in bepaalde banden vereist een diepte-investering ten aanzien van een andere manier van inzet en verdeling van dat spectrum: dynamisch spectrummanagement en medegebruik, ook wel **sharing** genoemd. Technologische ontwikkelingen als software-defined radio (SDR)[5] en block chain bieden steeds meer mogelijkheden voor een dergelijke paradigmashift. Hiertoe zijn we in 2022 een **pilot** gestart, die we in 2023 doorzetten. Het nut van deze ontwikkeling gaan we in internationaal verband verder uitdragen.

[5] Software-defined radio staat voor software-gedefinieerd radiosysteem. Dit is een radiocommunicatiesysteem waarin onderdelen die normaal gesproken geïmplementeerd zouden zijn in hardware (bijvoorbeeld mixers, filters, versterkers, etc.) nu worden uitgevoerd door middel van software op een pc of geïntegreerd systeem.

4 Gedragsbeïnvloeding en landelijke campagnes.

Het toezicht op de beschikbaarheid en de betrouwbaarheid van digitale infrastructuur en het gebruik daarvan vergt onze inzet, ook nadat het spectrum is verdeeld. Als rijksinspectie benaderen wij burgers, organisaties en bedrijven bij voorkeur in de **preventieve sfeer**: aan de voorkant oplossingen aandragen werkt effectiever dan achteraf corrigeren. We zetten in op passende interventies, gericht op het verbeteren en veranderen van gedrag. In 2023 vestigen we actief middels landelijke campagnes en doelgroep-voorlichting specifieke aandacht op de volgende onderwerpen:

- **Communicatiecampagne Chef Porto:**

Programmatische aanpak gericht op verbetering van het **landmobiele radiolandschap** door gedragsinterventies op systeemniveau. De focus ligt in 2023 op het activeren en empoweren van vergunninghouders via de voorlichtingscampagne: “Op zoek naar Chef Porto”;

- **Toezicht werkinstructie graafketen:**

Om de continuïteit van de essentiële diensten te borgen, is het van groot belang dat bij graafwerkzaamheden een adequate werkinstructie voor het graafteam beschikbaar is. Hierdoor wordt de kans op graafschades en daarmee de uitval van telecommunicatiediensten en diensten zoals de elektriciteitsvoorziening verkleind. De RDI houdt in 2023 extra toezicht op de meest omvangrijke zogenaamde grondroerders op het geven van een duidelijke werkinstructie aan het graafteam.

- **Dekking- en snelheidsverplichting:**

Voor de uitrol van mobiele telecommunicatiediensten op basis van de 5G-technologie zijn aan vergunningen voor de 700 MHz-band voorwaarden gekoppeld ten aanzien van de mobiele dekkings- en snelheidsverplichting (DSV). Dit borgt zowel de dekking als de snelheid, die met **mobiele netwerken** kan worden behaald. Medio 2022 is de DSV in werking getreden. Om naleving door de mobiele operators te realiseren, voert de RDI in 2023 in alle regio’s **controlemetingen** uit, waarbij we de meetresultaten openbaar publiceren.

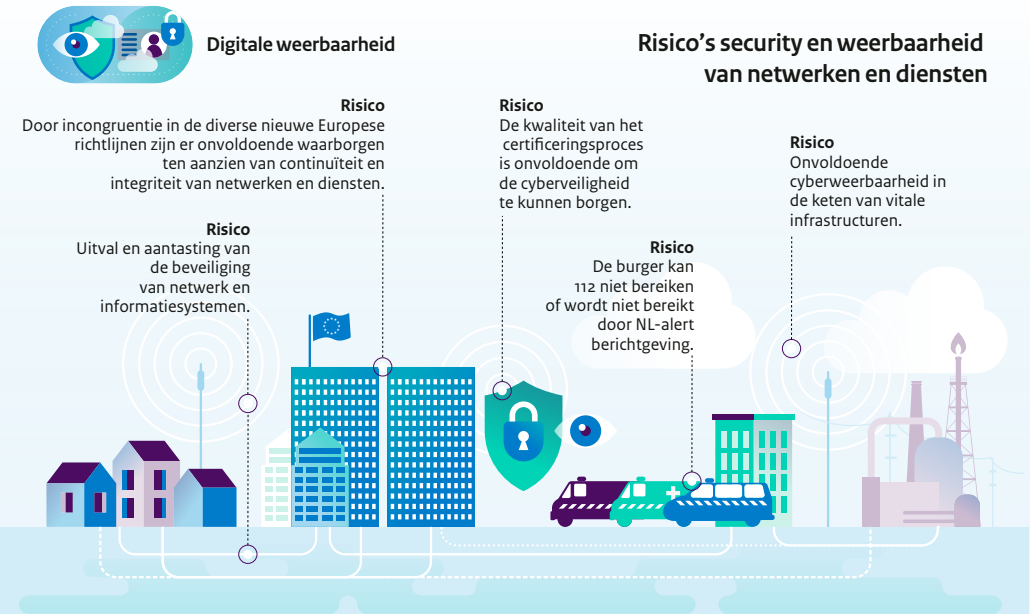
3.2 Security en weerbaarheid van netwerken en diensten

Maatschappelijk belang: Zijn de netwerken en diensten continu bereikbaar, integer en veilig?

In 2023 continueren we, op basis van de zorgplicht, het toezicht op **de continuïteit en integriteit van (telecom)netwerken en -diensten**. Dit doen we zowel vanuit het aspect van **telecomsecurity**. Netwerken dienen zo adequaat mogelijk beschermd te zijn tegen uitval en aantasting. Het kan daarbij bijvoorbeeld gaan om het alarmnummer 112 en de telecom, maar ook om de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. Nu de regelgeving op zowel Europees als nationaal is uitgebreid, zullen we ons toezicht daarop intensiveren. RDI ziet toe op de naleving van de borging van de cyberweerbaarheid van vitale infrastructuur door ondertoezichtgestelden. Daarnaast houden we, onder andere aan de hand van kwalificatie en certificering toezicht op **elektronische identiteiten** en **vertrouwensdiensten** en de **informatieveiligheid van telecommunicatiediensten**.

Verhoogde risico’s die zich voordoen in de security en weerbaarheid van netwerken en diensten zijn in drie categorieën in te delen. Dit zijn enerzijds risico’s die ontstaan door het gebruik van ongewenste systeemcomponenten in netwerken en anderzijds risico’s die ontstaan door onvoldoende cyberweerbaarheid in de keten van vitale infrastructuren. Daarnaast bestaat het risico dat door incongruentie in de nieuwe Europese regelgeving lacunes in de waarborgen ten aanzien van de continuïteit en integriteit van netwerken ontstaan.

In onderstaande figuur zijn de risico's weergegeven.



Speerpunten in 2023 ten aanzien van de security en weerbaarheid van netwerken en diensten zijn:

1 Implementatie NIS2, eIDAS2, CER en CSA regelgeving[6]

De Europese implementatie van de NIS2-, eIDAS2, CER- en CSA-regelgeving, alsmede de duiding van de contextafhankelijkheid met de CRA en AI-Act is een van de hoogste prioriteiten in 2023. Uiteraard geldt dit eveneens en nog in sterkere mate voor de **nationale implementatie** van bijbehorende regelgeving, in termen van **certificering en toezicht**. De Europese coördinatie vraagt om bijdragen vanuit de samenwerkende nationale en internationale toezichthouders, zodat waarborgen ten aanzien van de continuïteit en integriteit van netwerken en elektronische (internet) diensten standhouden.

2 Investeren in governance op systeemniveau en met technische kennis

Het belang van het **(stelsel)toezicht op de digitale weerbaarheid en security van vitale infrastructuren** neemt verder toe. De omvang van het toezicht zal fors stijgen waarbij diepgaande technische kennis en kennis van de governance en het systeem van groot belang zijn. "Onder de motorkap" van vitale digitale infrastructuren kunnen kijken blijft noodzakelijk om de weerbaarheid en security goed te kunnen beoordelen. De RDI zet hier ook in 2023 fors op in. Vanuit haar expertise en systeemoverzicht zal de RDI tevens investeren op de ontwikkeling van **guidance en kennisuitwisseling**, in samenwerking met collega toezichthouders, partners binnen de publieke sector, alsmede bedrijven en andere instellingen.

3 Structurele samenwerking toezichthouders

Een breed perspectief vanuit de diverse publieke belangen ten aanzien van security en weerbaarheid is noodzakelijk. Veiligheid is daarbij nevenschikkend aan andere publieke belangen, als economische levensvatbaarheid en bescherming van persoonsgegevens. De RDI kijkt vanuit het stelsel naar het versterken van de weerbaarheid, maar ook vanuit andere invalshoeken, zoals de responsinvalshoek. **Structurele samenwerking met collega toezichthouders in Nederland en Europa is essentieel**. De RDI zet in 2023 in op het uitbreiden en bestendigen van deze samenwerking.

[6] NIS2: Network and Information Security 2 (Richtlijn)
eIDAS2: Electronic Identities And Trust Services 2 (Verordening)
CER: Critical Entities Resilience (Richtlijn)
CSA: Cybersecurity Act (Verordening)
CRA: Cyber Resilience Act (Verordening)
AI-Act: Artificial Intelligence Act (Verordening)

4 Betrouwbaarheid informatiesystemen ten behoeve van de energietransitie

In hoofdstuk 2 van dit jaarplan is de gelijkloop van de digitale transitie en de energietransitie al naar voren gekomen. Een gecoördineerde aanpak van deze gelijkloop betekent een verbeterde kans op een **duurzame energievoorziening** door **digitale oplossingen** voor optimalisatie- en vertrouwensvraagstukken, een **verminderde afhankelijkheid** van energiemonopolies en een v**ermindering van de (cyber) kwetsbaarheid** van onze energievoorziening en onze Telecom/IT-infrastructuur. De RDI pakt hierbij haar rol als autoriteit in het digitaal domein door vroegtijdig **problemen te signaleren, vraagstukken te agenderen en oplossingen aan te dragen**. De RDI heeft hiervoor een speciaal programma Energietransitie opgestart dat in 2023 verder wordt vormgegeven. Zie hiervoor ook paragraaf 3.4.

5 Betrouwbaarheid en veiligheid internetverkeer borgen

De RDI zet in 2023 in op het effectief functioneren van de **netwerk- en transportlagen van het internet**. Dit doen we, samen met andere belanghebbenden, door het bevorderen van de implementatie van **relevante standaarden** en **best practices**. Er is onder meer aandacht voor routeringsecurity en verhogen van implementatiegraad van standaarden zoals Internet Protocol versie 6 (IPv6).

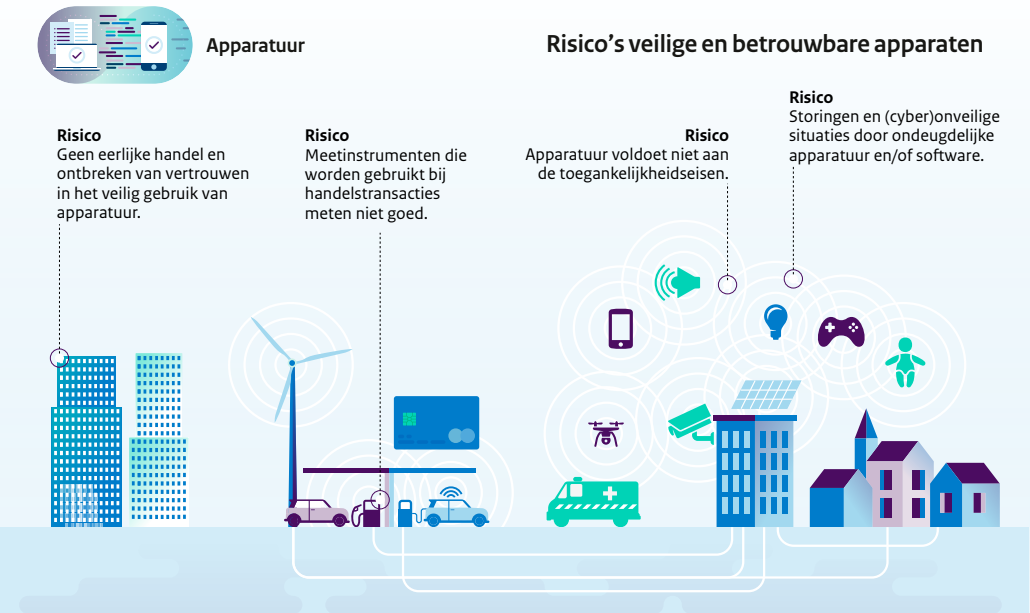
3.3 Veilige en betrouwbare apparaten

Maatschappelijk belang: Werken apparaten goed en veilig?

In toenemende mate vervagen de klassieke grenzen tussen soorten apparatuur. Veel apparatuur is inmiddels **draadloos verbonden** met het internet, wat **cyberrisico's** met zich meebrengt. Veel fysieke producten zijn daarbij, door de rol van software in deze producten, niet alleen een apparaat maar ook vaak een dienst. De **energietransitie** stimuleert het decentraal opwekken en gebruiken van energie en het gebruik van energiezuinige apparatuur. Echter hierdoor zien we vaker **storingen** in de ether. Onder invloed van de COVID pandemie is de productverkoop via e-commerce enorm gestegen.

Deze ontwikkelingen vragen om een verbrede benadering van de RDI waarbij samenwerking met collega toezichthouders en marktdeelnemers een belangrijke rol krijgt. **Normalisatie en standaardisatie** zijn hierbij aan de voorkant van groot belang. Bij het toezicht op het in het handelsverkeer brengen en het gebruik van apparaten, gaat het met name om eerlijke handel en het bevorderen van **vertrouwen in het veilig gebruik van apparatuur** die goed werkt. Dat gaat niet alleen maar om de apparaat-eigenschappen (ondeugdelijke constructie, werking, storingsgevoeligheid, elektromagnetische straling), de veilige werking en robuustheid tegen cyberdreigingen maar ook om betrouwbare hoeveelheidsinformatie van bijvoorbeeld weegschalen, kilowattuur meters en benzinepompen. Verder dient apparatuur te voldoen aan de toegankelijkheidseisen. Apparatuur dient immers ook bruikbaar te zijn voor mensen met een beperking.

In onderstaande figuur zijn de risico's op het gebied van veilige en betrouwbare apparaten weergegeven.



Speerpunten in 2023 ten aanzien van veilige en betrouwbare apparaten zijn:

1. Normalisatie en rol overheid

Het belang van overheidsdeelname aan normalisatie en standaardisatie neemt fors toe, zowel op Europees als op wereldniveau. Aan de voorkant problemen voorkomen beperkt de maatschappelijke impact van onzorgvuldig tot stand gekomen **normen en standaarden**. Niet alleen op de techniek zelf, maar vanuit diepgaande technische kennis op de kwaliteit van het voortbrengingsproces van normen en standaarden. Dit is nodig om **verborgen beïnvloeding** te voorkomen. Deze beïnvloeding kan ongewenste uitwerking hebben op marktposities en publieke belangen zoals veiligheid. De RDI continueert in 2023 haar rol in de normalisatie en standaardisatie continueren en breidt daar waar nodig uit.

2. Implementatie Europese regelgeving

De RDI focust zich in 2023 op de implementatie van de RED-regelgeving (Radio Equipment Directive) op het gebied van Digitaal Veilige Producten (DVP), waaronder IoT[7]-apparatuur. In een latere fase neemt de Cyber Resilience Act (CRA) dit aspect over. Het bestaande programma DVP breidt daarom uit met de duiding van de contextafhankelijkheid van de CRA met de CSA en de AI-Act. Binnen het bestaande AI-programma zetten we de **intensieve samenwerking** met de overige rijks- en markttoezichthouders voort onder de vlag van de Inspectieraad. Voor zowel de CRA als de AI-Act en de Toegankelijkheidsrichtlijn starten de voorbereidingen op de nationale implementatie. De Europese toezichtcoördinatie vraagt professionele bijdragen vanuit de samenwerkende toezichthouders via het Verbindingsbureau (SLO) en vanuit de sectorverantwoordelijkheid aan de diverse ADCO's (Administrative Cooperation Groups) en comités van de richtlijnen.

3. Breder perspectief productregelgeving

Een breed perspectief is noodzakelijk op de nieuwe ontwikkelingen vanuit de productregelgeving. Digitaal Veilige Producten, IoT en AI-toepassingen moeten we daarbij ook bezien vanuit invalshoeken als **cyberweerbaarheid** op systeemniveau, **continuïteit en bescherming van persoonsgegevens**.
De intensieve samenwerking met andere toezichthouders is van cruciaal belang om de publieke belangen samen adequaat te dienen. Door het veelal horizontale karakter van de nieuwe ontwikkelingen is iedere invalshoek in de digitale infrastructuur gelijktijdig aanwezig en relevant.

[7] IoT: Internet of Things

Aanvullend werken we intensiever samen met de markt om productsoorten te identificeren waarin naast cybergerelateerde ook andere **veiligheidsrisico's**, zoals elektrische veiligheid zijn gekoppeld. De Europese Markttoezichtsverordening is hiertoe richtinggevend en een belangrijke stimulans.

4. Gelijkloop digitale en energietransitie in relatie tot apparatuur

De reeds gesignaleerde en geagendeerde noodzakelijke gelijkloop van de digitale transitie en de energietransitie betekent eveneens een gecoördineerde aanpak van deze gelijkloop. Onze speerpunten daarbij zijn een duurzame energievoorziening door **digitale en metrologische oplossingen** voor **optimalisatie- en vertrouwensvraagstukken** en een **vermindering van de kwetsbaarheid** van onze energievoorziening. De focus in het werkprogramma ligt daarbij in 2023 op goedwerkende en veilige **energiemeters** en de verdere implementatie van **digitale meters** bij bedrijven en huishoudens. De RDI heeft hiervoor een speciaal programma Energietransitie opgestart dat in 2023 verder wordt vormgegeven. Zie hiervoor ook paragraaf 3.4.

3.4 Programma's Artificial Intelligence en Energietransitie uitgelicht

In deze paragraaf twee onderwerpen uitgelicht die, door hun bereik en impact, al onze thema's doorsnijden. Artificial Intelligence (AI) en de energietransitie zijn programma's die meerdere jaren voortduren en ook in 2023 beschikken over passende capaciteit en aandacht.

Artificial Intelligence

AI wordt steeds meer onderdeel van alle activiteiten in de maatschappij. En dus ook in de activiteiten waar de RDI (en andere toezichthouders) toezicht op houden. **Het toezicht op het gebruik van algoritmen bevindt zich in een opstartfase**.
AI toepassingen brengen nieuwe risico's en vraagstukken met zich mee. Dit geldt zeker toepassingen van AI in digitale apparatuur in het algemeen, en in netwerk- en informatiesystemen in het sectorspecifieke werkveld van de RDI (telecom, energie en internet) in het bijzonder. De RDI is bezig dit goed in beeld te krijgen, te bepalen welke expertise hiervoor nodig is en inspecteurs hierop voor te bereiden. Tevens zorgt de RDI voor eigen **AI toepassingen om de eigen dienstverlening te verbeteren**, maar ook om voldoende expertise in huis te hebben om adequaat toezicht te kunnen blijven houden op derde partijen.

Door de digitalisering raken de domeinen van verschillende toezichthouders elkaar en ook AI toepassingen worden in verschillende domeinen gebruikt. Het is van belang om te zorgen dat toezichthouders goed weten wie waar mee bezig is, waar je elkaar nodig hebt en samen kunt optrekken als dat gewenst is. De RDI besteedt veel tijd om dit samen met andere toezichthouders te realiseren.
Onder leiding van de RDI werken toezichthouders samen, wisselen ze kennis uit en zorgen ze dat er goede werkafspraken zijn. Ze ontwikkelen en delen expertise en capaciteit en geschikte methodes en andere tools. De RDI verricht in deze fase (2022 en 2023) werkzaamheden om de samenwerking en expertise van de RDI en de andere toezichthouders op AI te waarborgen. Het gaat om activiteiten omtrent **kennisontwikkeling, overleg met marktpartijen, ontwikkeling van standaarden en coördinatie tussen toezichthouders**.

Samenwerking op Europees niveau is noodzakelijk voor goed toezicht op basis van Europese regelgeving. De RDI is namens Nederland de initiatiefnemer van de Europese werkgroep van toezichthouders op AI. Die werkgroep, waarin ook ENISA[8] en de EC[w] zitten, heeft een vergelijkbaar doel als de Nederlandse samenwerking.

[8] ENISA: The European Agency for Cybersecurity

Energietransitie

De digitale transitie en de energietransitie zijn onlosmakelijk met elkaar verbonden, dit wordt ook wel de **twin transition** genoemd. Digitalisering geeft de mogelijkheid tot het verzamelen van accurate data over tijdstippen en locaties van opwek en verbruik van energie, en daarmee **inzicht** waardoor er o.a. efficiënter met (duurzame) energie omgegaan kan worden, vraag en aanbod beter gebalanceerd kan worden en hoe het elektriciteitsnet beter gemonitord wordt. De energietransitie is dus gebaat bij (meer en betrouwbare) digitalisering. Dit levert echter ook **potentiële cyberrisico's** op. Denk aan verminderde continuïteit van telecommunicatie, bewuste verstoringen in het elektriciteitsnetwerk en onveilig verbonden apparaten (omvormers, laadpalen en warmtepompen).

De RDI onderkent de twin transition en kijkt naar de kansen en risico's die dit voor de digitale infrastructuur oplevert. Zo houden we onder andere toezicht op: slimme meters en laadpalen op basis van de metrologiewet vanuit de directie apparatuur, graafwerkzaamheden (verzwaringen van het elektriciteitsnet) vanuit de directie infrastructuur en de cyberweerbaarheid van het elektriciteitsnet vanuit de directie digitale weerbaarheid. Dit alles met het doel om bij te dragen aan een **veilige digitale infrastructuur en een succesvolle energietransitie**.

Daarnaast doen we vanuit het programma energietransitie onderzoek naar nieuwe ontwikkelingen, bijvoorbeeld een verkenning van digitale platformen en de toepassing van AI in de digitale aansturing van onze elektriciteitssystemen. We zetten onze expertise in om nieuwe risico's en kansen te signaleren. Deze signalen gebruiken we op nationaal en Europees niveau voor kaderstelling, het ontwikkelen van normen en als input voor nieuwe wet- en regelgeving.

3.5 Onze aanpak en werkwijze

Met de ons ter beschikking staande informatie en analyses maken we op basis van risicoperceptie en -sturing keuzes. We duiden periodiek de maatschappelijke risico's per (sub)domein. Hiervoor hanteren we een werkwijze, waarbij we de prioriteitstelling in het toezicht onderbouwen en de maatschappelijke risico's scherp in de gaten te houden. **Een nul-risico samenleving bestaat echter niet**. Dit stimuleert ons om goed voorbereid te zijn op incidenten en de samenleving daarin te betrekken en mee te nemen.

Wij richten ons werk in volgens de lijnen van **basistoezicht, thematisch toezicht en incidenttoezicht**.
In ons **basistoezicht** gebruiken wij zoveel mogelijk data om met schaarse middelen goed toezicht te kunnen blijven houden. Een voorbeeld daarvan is ons maritieme toezicht dat voor het grootste deel is geautomatiseerd. Verder werken wij in ons basistoezicht steeds meer met steekproeven of monitoring om inzicht te houden in de stand van zaken. Komen daar signalen uit dan ga wij **thematisch** aan de slag: meestal waar naleving onvoldoende is, of waar het maatschappelijke risico en daarmee effect het grootst is. Alhoewel deze activiteiten niet als speerpunten in dit jaarplan worden genoemd, zijn ze van wezenlijk belang om grip te hebben en te houden in onze domeinen en een goede informatiepositie in stand te houden.
Incidenttoezicht laat zich niet plannen en vindt alleen plaats bij onvoorziene gebeurtenissen.
We onderzoeken hierbij acute verstoringen in de digitale infrastructuur met een hoge maatschappelijke relevantie. Storingen oplossen en het stimuleren van het voorkomen van dergelijke incidenten in de toekomst (systeemleren) staan hierbij centraal.

Dit geldt eveneens voor onze werkzaamheden als **kadersteller en vergunningverlener**. Een goed functionerend stelsel begint bij goede betrokkenheid bij de totstandkoming van kaders, op nationaal en internationaal niveau. Toelating tot een stelsel, door bijvoorbeeld het verlenen van vergunningen of registratie als een gekwalificeerde vertrouwensdienst is daarbij wezenlijk voor het goed functioneren van de digitale infrastructuur.
Tevens zetten we onze **onderzoeksagenda** in als instrument. Vraagstukken ten aanzien van maatschappelijke of technologische ontwikkelingen, trends of risico's die het werkveld van de RDI raken worden door verkennende, verdiepende of agenderende onderzoeken uitgevoerd.

4

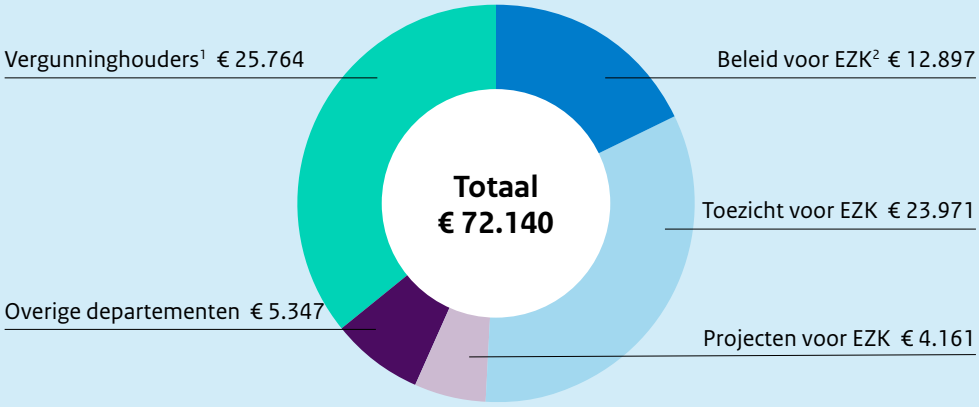
De RDI organisatie in cijfers

De RDI valt als **rijksinspectie en publieke dienstverlener** onder de verantwoordelijkheid van de Minister van Economische Zaken en Klimaat (EZK). Met onze activiteiten in uitvoering en toezicht voorkomen we in de kern risico's voor de samenleving, zoals deze zijn weergegeven in het vorige hoofdstuk. We kijken waar zaken verbeterd kunnen worden en spreken daarover met belanghebbenden en vertegenwoordigers van de samenleving.

Onze begroting voor 2023:

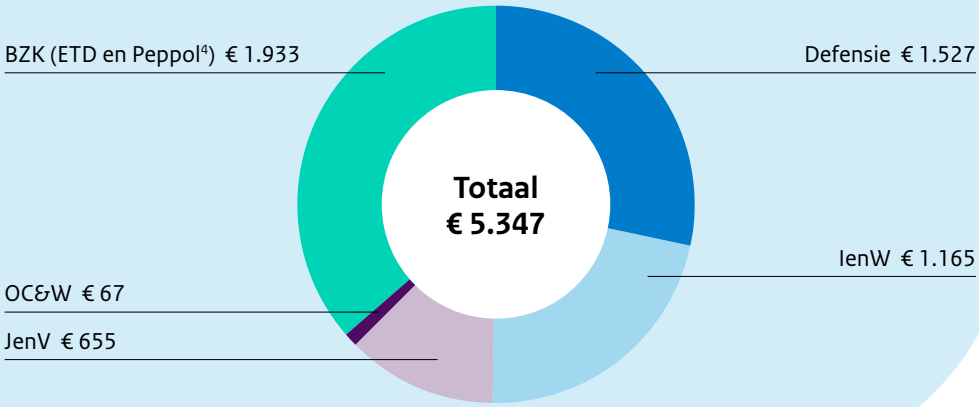
Omzet RDI 2023

Bedragen x 1.000



Omzet overige departementen[3]

Bedragen x 1.000



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

2 Beleid betreft vooral toelating en registratie van complexe vergunningen, voorbereiding en evaluatie van nieuw beleid, bijdragen aan nationale en internationale besluitvorming en de uitvoering van het Nationaal Antennebeleid.

3 Het betreft vooral inkomsten uit vergunningen ten behoeve van het gebruik van een specifiek, beschermd deel van het frequentiespectrum.

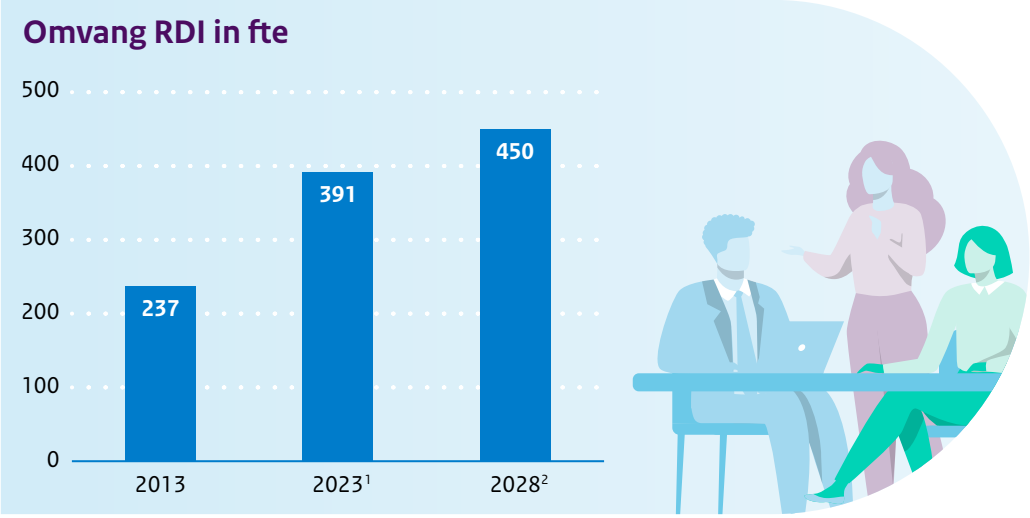
4 ETD = Elektronische ToegangsDiensten. Dit Afsprakenstelsel m.b.t. eHerkenning biedt een uniforme set van standaarden, afspraken en voorzieningen voor de geautoriseerde toegang tot digitale diensten. Peppol (Pan-European Public Procurement Online). Een Europese standaard waarmee snel, veilig en betrouwbaar elektronische berichten (zoals e-facturen) uitgewisseld kunnen worden.

Voor de RDI is het belangrijk 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 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.

Per 1 januari 2023 beschikt de RDI over bijna **400 formatieplaatsen**, waarvan zo'n 80 procent bestaat uit functies gericht op de primaire opdrachten als inspecteurs, analisten en specialisten, juristen en projectmedewerkers.

De organisatiegroei van de afgelopen jaren en de **verwachte groei** voor de toekomst is in onderstaande figuur weergegeven:



1 Groei is gevolg van vele nieuwe wet- en regelgeving op terrein van telecommunicatie en van de toenemende eisen die de samenleving stelt aan de telecommunicatie mogelijkheden.

2 Verwachte groei van het personeelsbestand als gevolg van nieuwe (toezichts)opdrachten n.a.v. de herziening van de Netwerk- en InformatieSystemen (NIS2), de Europese richtlijn voor Critical Entities Resilience (CER) en de Netcode. Besluitvorming vindt naar verwachting medio 2023 plaats.

Gezien de snelle ontwikkelingen in het werkveld van de digitale infrastructuur en de omvang van de beschikbare middelen en capaciteit maakt de RDI scherpe keuzes.
Het Jaarplan RDI 2023 geeft inzicht in die keuzes. In het **Jaarbericht** (terugkijkend) verantwoorden wij hoe wij ons toezichthoudende en uitvoerende taken hebben uitgevoerd.

Dit is een uitgave van:

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen

www.rdi.nl

T 088-0416000

Voor een veilig verbonden Nederland

Februari 2023 | Publicatienr. 22409383