Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Jaarplan Toezicht 2018

Agentschap

Telecom

Voorwoord

Telecommunicatie. Niet meer weg te denken uit onze huidige samenleving. Het is er altijd en overal. En dat moet ook, want we kunnen niet zonder. Dat geldt voor consumenten in het alledaagse leven. Maar zeker ook in professionele zin: telecommunicatie is randvoorwaardelijk voor onze veiligheid en economie en biedt interessante toepassingen en kansrijke mogelijkheden voor bijvoorbeeld de healthsector, het onderwijs of de zorg. Betrouwbare en beschikbare IT/telecommunicatienetwerken en andere technische infrastructuren. Dat is waar Agentschap Telecom voor staat. En dat is waar het toezicht van Agentschap Telecom zich op toespitst.

Als toezichthouder handelt het agentschap altijd vanuit het publieke belang. Dit jaarwerkplan beschrijft de wijze waarop Agentschap Telecom dat in 2018 vorm geeft. Het bevat een beschrijving van relevante ontwikkelingen binnen de domeinen waarop het agentschap toezicht houdt. Het benoemt vanuit de publieke belangen en bijbehorende risicoanalyse de gekozen prioriteiten voor 2018.

We zien dat de maatschappij in toenemende mate eisen stelt aan de dekking en continuïteit van netwerken. Bereikbaar zijn wordt steeds meer ervaren als een levensbehoefte. Agentschap Telecom zet zich in voor de optimalisatie van de dekking en het bereik van mobiele telecomnetwerken. Vanuit de rol als toezichthouder geven we bijvoorbeeld tijdig duidelijkheid over de ingebruikname verplichtingen voor nieuwe frequenties voor mobiele netwerken, doen we lokaal onderzoek in gemeenten naar de bereikbaarheid van 1-1-2 en onderzoeken we de werking van NL-Alert:. Ook is er aandacht voor de werking van lokale draadloze bedrijfs-communicatienetwerken die vaak cruciaal zijn voor het veilig en efficiënt uitvoeren van bedrijfsprocessen. Naar verwachting zullen wij steeds meer inzet moeten plegen op dit specifieke deel van de technische infrastructuur, de mobiele telecommunicatie met de bijbehorende extra benodigde financiële randvoorwaarden. Daarnaast staan wij vanuit de rol als uitvoerder stil bij de nodige randvoorwaarden voor de uitrol van 5G.

Het jaar 2018 zal ook voor een belangrijk deel in het teken staan van de nieuwe digitale infrastructuren en het creëren van vertrouwen in de digitale samenleving die daarmee ontstaan is. Agentschap Telecom houdt toezicht op aanbieders van elektronische vertrouwensdiensten en toegangsdiensten. Vanuit die verantwoordelijkheid ziet het agentschap toe op de veiligheid en betrouwbaarheid van 'vertrouwensdiensten', zoals elektronische handtekeningen, elektronische zegels of de authenticatie van websites en bijvoorbeeld de betrouwbaarheid van eHerkenning. Daarmee ondersteunen we het vertrouwen dat burger en bedrijf mogen en moeten hebben in de digitale dienstverlening. Agentschap Telecom werkt bovendien aan het ontwikkelen van toezichtbeleid voor de informatieveiligheid van een aantal vitale infrastructuren in het kader van de Cybersecuritywet.

2018 staat wederom in het teken van de leveringszekerheid van vitale diensten (zoals energie en telecom). Door middel van het toezicht op de Wibon willen we samen met de graafsector de graafschades sterk te laten verminderen. Code "oranje" moet positief omgebogen worden.
Als toezichthouder op de Metrologiewet zien we er op toe dat slimme energiemeters feilloos werken. En dat moet vanzelfsprekend ook gelden voor alle draadloze verbindingen die hiervoor nodig zijn. Leveringszekerheid en de goede werking van de technische infrastructuur dragen bij aan het vertrouwen van de burger in de energie-infrastructuur. En dat vertrouwen is cruciaal voor het slagen van de komende energietransitie.

Het jaar 2018 belooft interessant en uitdagend te worden. Dat is het nu al.
Agentschap Telecom staat voor de beschikbaarheid en betrouwbaarheid van IT- en communicatienetwerken,
zodat Nederland veilig verbonden is.

Inhoud

Inleiding

Agentschap Telecom werkt als overheidsorganisatie aan maatschappelijke belangrijke vraagstukken. We houden ons als uitvoerder én toezichthouder bezig met vragen die iedereen in het dagelijks leven raken:

- Mijn appje komt even niet aan, maar naar 112 kan ik toch altijd bellen?
- Krijg ik wel echt een kilo appelen of 15 liter benzine?
- Is mijn slimme energiemeter wel betrouwbaar?
- Koop ik nu een apparaat dat tegen storing bestand is?
- Ze zijn aan het graven in mijn straat, heb ik straks nog wel gas en stroom?
- Mooi geluid uit die digitale radio; kan ik die straks ook in Appelscha ontvangen?
- Hoe weet ik of ik mijn gegevens betrouwbaar naar een website stuur?
- Koop ik nu wel een echt gouden ring?
- Hoe is het mogelijk dat ik kan bellen met mijn dochter die op missie is in Afghanistan?
- Is die antenne wel veilig die net op de hoek van de straat is neergezet?

Allemaal terechte maatschappelijke vragen en zorgen rondom de beschikbaarheid en de betrouwbaarheid van IT-, communicatie-, en andere technische netwerken die we dagelijks tegen komen. Of het nu mobiel dataverkeer, wifi in en om het huis, kabeltelevisie, veilig betalen via internet,

graven in de buurt van gasleidingen of de werking van weegbruggen bij de afvalstort betreft.

Beschikbaarheid gaat dan over het storingsvrij kunnen werken en het fysiek veilig kunnen gebruiken van de apparaten en netwerken. Betrouwbaarheid is hierbij het continu, zonder manipulatie en informatieveilig gebruiken van de netwerken.

Beschikbaarheid en betrouwbaarheid van deze technische infrastructuur zijn in de beleving van burgers een levensbehoefte geworden. Zonder deze technische infrastructuur loopt ons dagelijks leven vast en stagneert de economische groei.

Onze missie is daarom:

Agentschap Telecom waarborgt de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken.

Het voorliggende werkprogramma geeft de prioriteiten voor 2018 weer in de rol van toezichthouder, die vanuit deze missie verantwoordelijk is voor het toezicht op (onderdelen van) de Telecommunicatiewet, de Metrologiewet, de Waarborgwet, de Wet Informatieuitwisseling Ondergrondse Netwerken, de eIDAS-verordening, het ETD-stelsel, de Cybersecuritywet en de Wet Ruimtevaartactiviteiten. We werken vanuit de principes van informatiesturing en risicogerichtheid. Daarnaast vormen de principes uit de Kaderstellende Visie op Toezicht een belangrijke leidraad voor ons denken en handelen. De focus voor de komende jaren ligt op de verdere ontwikkeling van de reflectieve functie van het toezicht door tijdig belangrijke issues te signaleren en te agenderen.

Agentschap Telecom is een onderdeel van het ministerie van Economische Zaken en Klimaat. Het agentschap heeft vestigingen in Groningen en Amersfoort.

1 Toezichtdomein, op wie en wat houden we toezicht?

Agentschap Telecom kent een breed toezichtdomein met één grote gemeenschappelijke noemer. Het toezicht ziet in nagenoeg alle deeldomeinen toe op technische infrastructuren die in het dagdagelijkse functioneren van onze maatschappij een belangrijke betekenis hebben. Onze rol gaat verder dan alleen de telecom- en IT-infrastructuren. Zo vallen onder andere ook de meet-en weeginfrastructuur onder deze notie, net als de ondergrondse kabel- en leidingeninfrastructuur en de digitale infrastructuur.

1.1 Toezicht op de goede werking van technische infrastructuren

Bij het toezicht op de goede werking van technische infrastructuren gaat het om publieke belangen zoals een veilig en storingsvrij gebruik van telecom- en omroepnetwerken, de beschikbaarheid en bruikbaarheid van infrastructuren, eerlijke handel en bescherming van burger en consument tegen manipulaties van technische infrastructuren en ondeugdelijke apparaten. Burger en bedrijf moeten kunnen vertrouwen op de goede werking van de infrastructuur.

1.1.1 Veilig en storingsvrij gebruik van apparatuur

Bij het gebruik van apparatuur voor allerlei toepassingen gaat het om veilig gebruik zonder storing van en op anderen. Verstoring kan plaatsvinden door

verkeerd gebruikte apparatuur of ondeugdelijke apparatuur. Er kan ook sprake zijn van illegaal gebruik. De gebruikte apparatuur moet ook elektrisch veilig te gebruiken zijn. Daarom zijn er tal van (inter)nationaal bepaalde eisen en Europese richtlijnen, zoals de EMC-richtlijn en de RED, waaraan voldaan moet worden om veilig en storingsvrij gebruik van elektrische en elektronische apparatuur te garanderen. Niet veilig gebruik kan doordat apparatuur bijvoorbeeld limieten voor het zendvermogen overschrijdt. Ook hier gelden internationale eisen.

Agentschap Telecom houdt hier toezicht op via onder andere nalevingstoezicht, markttoezicht, thematische onderzoeken en het behandelen van storingsklachten.

1.1.2 Beschikbare en bruikbare netwerken in de ether en in de grond

Om te zorgen dat draadloze netwerken voor telecommunicatie en transportnetwerken van vitale diensten beschikbaar zijn en bruikbaar blijven, is het van belang dat partijen zich houden aan de eisen die van toepassing zijn op het netwerk. Voor draadloze netwerken en toepassingen gelden er voorschriften en beperkingen op grond van de Telecommunicatiewet, opgenomen in zendvergunningen of algemeen verbindende voorschriften. Hierdoor kunnen de diverse netwerken naast elkaar blijven functioneren. Voor ondergrondse transportnetwerken zijn er vanuit de Wet Informatieuitwisseling Ondergrondse Netwerken eisen gesteld aan de diverse partijen die een rol vervullen in de graafketen. Door het beperken en terugdringen van het aantal graafschades wordt de leveringszekerheid van gas, water en licht veilig gesteld.

Agentschap Telecom houdt hier toezicht op via onder andere nalevingstoezicht op de draadloze netwerken en toepassingen. En in de graafketen via nalevingstoezicht, incidentonderzoek en handhavingscommunicatie.

1.1.3 Eerlijke handel

Om eerlijke handel te bevorderen, dient de technische infrastructuur op het gebied van meten en wegen te voldoen aan de eisen uit de Metrologiewet. Niet alleen de consument, maar ook de tussenhandel moet er op kunnen vertrouwen dat men "waar krijgt voor het geld". Dit geldt ook voor het gehalte aan edelmetaal in bijvoorbeeld sieraden. De vereisten van de Waarborgwet zijn hierop van toepassing.

Agentschap Telecom houdt hier toezicht op via onder andere nalevingstoezicht en marktToezicht.

1.2 Toezicht op het vertrouwen in digitale infrastructuren

Bij het toezicht op het vertrouwen in digitale infrastructuren gaat het om publieke belangen zoals de continuïteit van telecomnetwerken en van hoge antenne-opstelpunten. En het kunnen hebben van digitaal vertrouwen door betrouwbare elektronische identiteiten en certificaten en het op orde zijn van de cybersecurity van vitale infrastructuren. Burger en bedrijf moeten vertrouwen kunnen hebben in het veilig gebruik van de infrastructuur.

1.2.1 Continuïteit van telecomnetwerken en hoge antenneopstelpunten

Vaste en draadloze telecomnetwerken moeten naast storingsvrij werken ook een hoge beschikbaarheidsgraad hebben. Dat laatste geldt ook voor niet eenvoudig dupliceerbare hoge antenne-opstelpunten. Continuïteit is daarbij een cruciaal

publiek belang dat in de Telecomwet is geregeld. Mede in verband met de elkaar snel opvolgende technische ontwikkelingen en de steeds hogere verwachtingen van burger en bedrijf is hier sprake van open norm wetgeving.

Agentschap Telecom houdt hier toezicht op via systeemtoezicht en nalevingstoezicht. Een belangrijk instrument om voor specifieke publieke belangen een gesloten norm te laten overwegen, is het signaleren en agenderen van een dergelijke behoefte door middel van een incidentonderzoek of een thematisch onderzoek.

1.2.2 Vertrouwensdiensten en certificaten

Elektronische vertrouwensdiensten zijn diensten die het vertrouwen in online transacties bij bedrijven en consumenten vergroten. Hiervoor geldt Europese wetgeving, de eIDAS verordening. Door gebruik van vertrouwensdiensten kan men veilig online diensten afnemen of digitaal zaken met bijvoorbeeld de overheid regelen.. Ook regelt eIDAS het grensoverschrijdend gebruik van nationale elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de EU. Zo wordt het gemakkelijker om online en over de grens zaken te doen . Het gaat hierbij om onder andere digitale certificaten voor elektronische handtekeningen en voor de authenticiteit van websites Agentschap Telecom houdt hier toezicht op en is verantwoordelijk voor het toelaten van partijen op de lijst van zogenaamde Trusted Service Providers die gekwalificeerde vertrouwensdiensten mogen leveren.

Daarnaast is er het ETD-stelsel, het afsprakenstelsel elektronische toegangsdiensten, waar onder andere eHerkenning valt. Dit is een gestandaardiseerd inlogsysteem waarmee organisaties hun diensten veilig online toegankelijk kunnen maken. In essentie regelt eHerkenning de digitale herkenning (authenticatie) en controleert het de digitale bevoegdheid (autorisatie) van iemand die online een dienst wil afnemen. Ondernemers, consumenten en ambtenaren loggen met hun eHerkenningsmiddel, het inlogmiddel, in op een webdienst van een aangesloten organisatie en kunnen zo online hun zaken regelen. eHerkenning is één van de voorzieningen die samen de generieke digitale infrastructuur voor de e-overheid vormen. Het is nu nog een stelsel met privaatrechtelijke afspraken maar komt naar verwachting met de Wet Digitale Overheid onder publiekrechtelijk toezicht van het agentschap.

Agentschap Telecom voert tot aan de inwerkingtreding van de Wet Digitale Overheid het toezicht uit waarbij een Commissie van Deskundigen op basis van de toezichtsbevindingen de staatssecretaris van BZK adviseert over de te nemen maatregelen richting de betreffende partij binnen het Afsprakenstelsel. Na inwerkingtreding van de Wet Digitale Overheid treedt de Commissie terug en voert Agentschap Telecom systeemtoezicht uit op een publiekrechtelijke basis.

1.2.3 Cybersecurity

Met de Cybersecuritywet (Csw) wordt de Europese Netwerk InformatieBeveiligingsrichtlijn geïmplementeerd in de Nederlandse wetgeving. Het doel van deze richtlijn is om te waarborgen dat in essentiële sectoren binnen de Unie de netwerk- en informatiebeveiliging op een hoog minimum niveau komt. Alle organisaties die onder de Csw vallen, komen onder toezicht te staan en krijgen daarbij tevens een meldplicht voor het melden van veiligheidsincidenten bij het NCSC en de toezichthouder. Agentschap Telecom wordt aangewezen als toezichthouder voor de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. Agentschap Telecom houdt na inwerkingtreding van de Csw toezicht via systeemtoezicht.

1.3 Toezicht op specials

Het toezicht op specials is ondergebracht bij Agentschap Telecom in verband met de benodigde technisch/bestuurlijke kennis en/of op grond van het voorkomen van onnodige versnippering van toezichttaken in combinatie met een groep ondertoezichtgestelden die reeds onder het toezicht staan van het agentschap.

Het toezicht op specials betreft:

- Het toezicht in het kader van de Wet Ruimtevaart Activiteiten. Partijen die onder Nederlandse jurisdictie een object de ruimte in willen brengen, moeten aan eisen voldoen. Dit om schade-aansprakelijkheid van de Nederlandse Staat te voorkomen ten gevolge van de lancering, het verblijf in de ruimte en de terugkeer in de dampkring van het betreffende object, veelal een satelliet.
- Het toezicht op de vereisten van de Kijkwijzer.
- Het toezicht op de inhoudelijke eisen die verbonden zijn met vergunningen voor radio-omroep. Dit zijn aanvullende eisen bovenop de Mediawet en zijn onder de Telecommunicatiewet verwerkt in de telecomvergunningen. Het gaat hierbij om de eisen ten aanzien van regiogerichtheid van Niet Landelijke Commerciële Omroepen en de eisen ten aanzien van geclausuleerde FM-kavels van Landelijke Commerciële Omroepen.

2 Welke ontwikkelingen zien we in ons toezichtdomein?

Agentschap Telecom is naast toezichthouder ook beleidsuitvoerder. Vanuit beide rollen monitoren en duiden we de ontwikkelingen in ons werkveld. De focus ligt op de ontwikkelingen die het risicobeeld in onze toezichtdomeinen kunnen beïnvloeden. Een belangrijk instrument dat we gebruiken is de ECD-radar[1]. Deze radar geeft visueel weer welke ontwikkelingen in het Elektronische Communicatie Domein en de overige werkvelden op welke termijn relevantie hebben voor ons werk. Met de ons jaarbericht de Staat van de Ether[2] blikken we jaarlijks terug.

Vanuit de ontwikkelingen in de diverse werkvelden zien we de volgende focuspunten voor ons toezicht:

Technische infrastructuren als levensbehoefte

- De druk op de beschikbare mobiele capaciteit en bereik vanuit de samenleving neemt toe. Niet alleen

[1] https://www.agentschaptelecom.nl/onderwerpen/onderzoek-en-ontwikkelingen/trends-in-beeld-de-ecd-radar
[2] https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/index

is de bereikbaarheid van 1-1-2 via onze smartphone belangrijk, ook is gewenst dat we de smartphone altijd en overal kunnen gebruiken.

- Het ingezette beleid om steeds meer draadloze toepassingen vergunningvrij te kunnen gebruiken, is blijvend succesvol en dringt volledig door in ons dagelijks leven. Ons huishouden draait steeds meer op het gebruik van deze toepassingen die ook nog eens met het internet verbonden zijn. Het Internet of Things (IoT) breidt gestaag uit.
- Tegelijkertijd zijn onze vitale infrastructuren fysiek kwetsbaar als gevolg van onzorgvuldig handelen (onder ander door graafschades en storingen) of als gevolg van crimineel handelen (onder andere door illegale netwerkversterkers of illegaal stroom aftappen ten behoeve van clandestiene omroepuitzendingen).

Technische infrastructuren zijn complex

- Door de verder en vergaande functionele integratie van traditionele telecomnetwerken met internet en media is de complexiteit van technische infrastructuur toegenomen. Dit betekent dat bij verstoringen van netwerken specialistische kennis nodig is om tot oplossingen te komen. Deze kennis is minder toegankelijk voor bedrijf en burger waardoor ook het handelingsperspectief bij verstoring beperkt wordt.
- Digitalisering en modernisering zet ook door op traditionele markten. Voorheen eenvoudige communicatiesystemen, zoals het gebruik van de marifoon voor de veiligheid op het water, worden complexer in gebruik en onderhoud door bijvoorbeeld aanvullende digitale systemen ten behoeve van identificatie (ATIS, AIS).

Toezicht op vertrouwen in digitale infrastructuren

- De ontwikkeling van de overheidsaandacht voor digitaal vertrouwen kan worden gemodelleerd aan de hand van een waterdruppel die in een poel valt en waterrimpels veroorzaakt in de vorm van ringen (zie hiervoor de afbeelding op pagina 9). De druppel symboliseert een technische uitvinding, deze veroorzaakt een golf in de vorm van een ring. Iedere ring/golf symboliseert een majeure technische ontwikkeling. Iedere nieuwe ontwikkeling (golf/ring) bouwt voort op de voorgaande.
- Iedere majeure technische ontwikkeling leidt tot nieuwe toepassingen en gebruik van die techniek. Deze nieuwe toepassingen en gebruik hebben maatschappelijke gevolgen. Met iedere nieuwe golf/ring wordt de omvang van de maatschappelijke gevolgen groter. De maatschappelijke gevolgen kunnen ertoe leiden dat publieke belangen in het geding zijn. Dit kunnen reeds gedefinieerde publieke belangen zijn zoals privacy, maar ook nieuwe publieke

belangen die nog niet als zodanig zijn gedefinieerd. Vaak gaat het echter over belangen die al wel gedefinieerd waren, maar in de context van de techniek een nieuwe connotatie krijgen. Zoals (internet)privacy, (cyber)veiligheid.

- Dit heeft geleid tot een uitbreiding van het werkveld van toezicht taken, zoals het toezicht op eIDAS, op ETD als voorloper op de wet Digitale Overheid, op de Cybersecuritywet (NIB-richtlijn) en het toezicht op de continuïteit van telecomnetwerken en hoge antenneopstelpunten.
  Het toezicht in deze nieuwe werkvelden is veelal open norm toezicht.

Toezicht over de grens

- De globalisering van de markt voor (telecom)apparatuur zet verder door. Hoewel de interne Europese markt nog leidend is voor de afstemming van toezicht over de grens, worden globale ontwikkelingen steeds belangrijker. De handel via internet draagt hier fors aan bij.
- Voor de nieuwe werkvelden van Agentschap Telecom / Toezicht, zoals het toezicht op de eIDAS-regelgeving, is Europese samenwerking een must. Digitaal vertrouwen ontstaat en stopt niet bij een staatsgrens.

Transparant Toezicht

- De reflectieve functie van het toezicht wordt essentieel om tijdig en effectief maatschappelijk relevante vraagstukken te signaleren en te agenderen. Reactief en repressief optreden is nog steeds nodig,. Echter om problemen voor te zijn en risico's te verminderen moet de toezichthouder aan de voorkant van de problematiek komen en zorgen dat er al mensen en middelen klaar staan op het moment dat het echt nodig is.
- Het verantwoord gebruik van Big data en open data wordt cruciaal voor de te maken keuzes en de af te leggen verantwoording.

3 Welke prioriteiten stellen we in 2018?

Op basis van de in hoofdstuk 2 geschetste ontwikkelingen, de bijbehorende risicoduiding, signalen uit de markt en analyses kiezen we onze prioriteiten, naast het uit te voeren basistoezicht. We werken informatiegestuurd en risicogericht met als doel de publieke belangen te beschermen en maatschappelijke risico's te verminderen.

3.1 Technische infrastructuren als levensbehoefte

Publiek belang ⇨	Doel ⇨	Output/actie
Optimalisatie van de dekking en het bereik van mobiele telecomnetwerken	Het toezicht op de ingebruikname verplichting (IGV) en de dekkingsplicht uit de te veilen vergunningen voor mobiele communicatie in de 700 MHz-band voorbereiden en kenbaar maken aan de (potentiele) stakeholders om de markt en	Transparant meetprotocol met eenduidige eisen en meetmethodiek Vastellen benodigde uitbreiding toezichtcapaciteit

	maatschappij voor te bereiden op de verplichtingen en aanpassingen van de dekking van mobiele telecomnetwerken	
Leveringszekerheid van vitale diensten (zoals energie en telecom) bevorderen door graafschades te beperken	De in 2017 door Agentschap Telecom afgegeven "code oranje" ten aanzien van de oplopende aantallen graafschades gebruiken om de graafsector het aantal graafschades sterk te laten verminderen.	Plan van aanpak door de markt laten opstellen en implementatie monitoren Fysieke inspecties ter verhoging van de pakkans van niet-nalevers Extra aandacht voor de opdrachtgevers van graafwerkzaamheden
(Dreigende) verstoring van vitale delen van diverse infrastructuren door crimineel handelen rond illegaal frequentiegebruik verminderen	Het verkrijgen van inzicht in de drijfveren van groepen etherpiraten om tot crimineel gedrag te komen en handelingsperspectieven ontwikkelen om dit verder en effectiever tegen te gaan	Thematisch onderzoek naar effectief optreden in het kader van het optreden Bescherming Omroep Frequenties
Vertrouwen van de burger in de toekomstige energietransitie vergroten	Het signaleren en agenderen van mogelijke toekomstige zwaktes in het decentraliserende energie systeem met bijbehorende mitigerende handelings-perspectieven	Thematisch onderzoek in het kader van de energietransitie
Vertrouwen van de burger in de overheidsalarmering in	Het toetsen van de werking van NL-Alert in openbare mobiele telecomnetwerken	Audits bij de operators naar opzet, bestaan en

het geval van rampen en crises vergroten		werking Afspraken over herstel van eventuele bevindingen
Opheffen verstoringen bij vitale overheidsdiensten bij ernstige bedreigingen van hun taakuitvoering	Het operationeel stellen van de nieuwe Beschikbaarheids- en BereikbaarheidsDienst (BBD) vanuit de opdracht uit de Nota Frequentiebeleid 2016	Operationele BBD conform de opgestelde beleidsregel en een stabiel BBD-rooster Oefen, trainings en opleidings (OTO)-programma om geoefendheid BBD te garanderen
Bevorderen van de beschikbaarheid van telecomnetwerken om het maatschappelijk leven geen hinder te laten ondervinden van onnodige uitval	Het opstellen van de stand van zaken van de uitwerking van de ENISA guidelines voor continuïteit van telecomnetwerken bij de ondertoezichtgestelde telecomoperators	Thematisch onderzoek met stand van zaken en aanbevelingen voor eventueel te nemen maatregelen
Na de branden in de hoge telecommasten bij Smilde en Lopik het risico verminderen op het uitvallen van de cruciale, niet dupliceerbare delen van de telecominfrastructuur op aangewezen hoge antenne-opstelpunten	Het effectief en efficiënt uitvoeren van het toezicht op de continuïteit van hoge antenne-opstelpunten	Implementatie van het toezichtarrangement Nulmeting op de in de AMVB geduide hoge opstelpunten

3.2 Technische infrastructuren zijn complex

Publiek belang ⇨	Doel ⇨	Output/actie
De digitalisering van de omroep geeft meer keuze	De uitrol van de digitale omroepnetwerken laten	Uitvoeren IGV-metingen volgens

aan consument en betere kwaliteit	plaatsvinden conform de in de vergunning opgenomen eisen voor de ingebruikname verplichting (IGV) voor Digitale Audio Broadcast (DAB)	een kenbaar gemaakt meetprotocol en eventueel opvolgende handhavende acties
Bevorderen van het vertrouwen van de consument in de betrouwbaarheid van de levering van energie om de overgang naar elektrisch rijden mede te ondersteunen	Inventariseren van de noodzakelijke overheidsbemoeienis bij de opzet en werking van laadpalen voor elektrische voertuigen in het openbare domein	Thematisch onderzoek met aanbevelingen en handelings-perspectieven
Verminderen van de potentiele storingsproblematiek die het gevolg is van de exponentiele toename van elektrische en elektronische apparatuur in onze directe leefomgeving	Ontwikkelen van mogelijkheden om de negatieve effecten te kunnen bestrijden van zogenaamde Man Made Noise en met name de in-house problematiek	Thematisch onderzoek met aanbevelingen en handelings-perspectieven
Vroegtijdig problemen in de samenwerking/samenleving tussen telecomsystemen oplossen, die ondanks naleving van alle voorschriften zijn ontstaan en niet op te lossen zijn met het reguliere regulerende instrumentarium	Het effectief kunnen invullen van de nieuwe rol van toezicht als bemiddelaar en arbiter vanuit de opdracht in de Nota Frequentiebeleid 2016	Rolbeschrijving van zowel bemiddelaar als arbiter met de bijbehorende duiding van de benodigde bevoegdheden, capaciteit en middelen
De kwaliteit van telecomnetwerken in cruciale bedrijfsprocessen verbeteren en de afhankelijkheid daarvan verminderen	Onderzoeken of een gebiedsgerichte benadering vanuit het toezicht de risico's van telecomafhankelijkheid in cruciale bedrijfsprocessen	Thematisch onderzoek met aanbevelingen, handelings-perspectieven en een behoefte-

	kan verminderen. De aanleiding is de slechte naleving bij BRZO-bedrijven	stelling uitbreiding toezichtcapaciteit

3.3 Toezicht op het vertrouwen in de digitale infrastructuur

Publiek belang ⇨	Doel ⇨	Output/actie
Nederland moet kunnen vertrouwen op digitale dienstverlening en digitale identiteiten	Het omzetten van het huidige toezicht op basis van het Afsprakenstelsel naar het publiekrechtelijk toezicht op basis van de wet Digitale Overheid	Uitvoeren van het plan van aanpak voor de ombouw van de ondersteuning van de Commissie van Deskundigen naar een eigenstandige publiek-rechtelijke uitvoering van het toezicht
Vitale infrastructuren moeten hun informatiebeveiliging goed op orde hebben om de leveringszekerheid van vitale processen en diensten zeker te stellen	Het effectief invullen van het toezicht op de Cybersecuritywet voor de voor EZK aangewezen vitale diensten en infrastructuren	Inrichting van het toezicht inclusief meldloket
Nederland moet kunnen vertrouwen op digitale elektronische transacties	Het borgen van een accuraat beveiligingsniveau van (verleners van) vertrouwensdiensten	Opstellen toezichtkalender met thema-inspecties bij gekwalificeerde verleners van vertrouwensdiensten Informatiecampagne richting publiek en niet-gekwalificeerde verleners van vertrouwensdiensten

3.4 Toezicht over de grens

Publiek belang ⇨	Doel ⇨	Output/actie
Bevorderen van het vrij verkeer van goederen op een wijze die recht doet aan de belangen van het voorkomen van storing en het veilig kunnen gebruiken van apparatuur	Het verhogen van de awareness bij fabrikanten en importeurs/handelaren van het belang van het naleven van Europese richtlijnen inzake apparatuureigenschappen	Het uitvoeren van het actieplan Markttoezicht van de onder de Inspectieraad ressorterende Alliantiewerkgroep
Bevorderen van het consumentenvertrouwen in Europese regelgeving rond de veiligheid van apparatuur	Meningsvorming over de kwaliteit van certificerende instellingen (NOBO's) in relatie tot hun bijdrage aan het doel van de betreffende regelgeving	Leveren van de gewenste bijdrage aan het rapport van de Inspectieraad
Bevorderen van het consumentenvertrouwen in de handel van apparatuur buiten de reguliere nationale afzetkanalen om	Het effectief bestrijden van de invoer en verkoop van non- conforme apparatuur (op de markt via internet en e-commerce)	Thematisch onderzoek met aanbevelingen en handelings-perspectieven Informatiecampagne richting consument

3.5 Transparant toezicht

Publiek belang ⇨	Doel ⇨	Output/actie
Feitelijke onderbouwing van de keuzes van het toezicht en de uitvoering en de bijbehorende verantwoording uitbouwen om het vertrouwen van de burger in de overheid te bevorderen	Het effectief inzetten van de data-analysecapaciteit voor de feitelijke onderbouwing van gemaakte keuzes	Uitbreiding van de data-analyse-capaciteit van Toezicht binnen de bestaande formatie Door ontwikkelen van de analyse-

		tooling
De publieke belangen van de Metrologiewet en Waarborgwet borgen volgens de inzichten van modern toezicht	Het vanuit de verstatelijking van Verispect overgenomen toezicht op de naleving van de Metrologiewet en de Waarborgwet in overeenstemming brengen met de toezichtvisie van Agentschap Telecom, met behoud van de sterke punten van het huidige toezicht	Opstellen en implementatie meerjarig veranderplan

4 Wat is de basis van ons toezicht?

Agentschap Telecom houdt onder politieke verantwoordelijkheid van de staatssecretaris van Economische Zaken en Klimaat toezicht op de goede werking van technische infrastructuren en op het vertrouwen in digitale infrastructuren. Toezicht heeft als hoofddoel om publieke belangen te beschermen en maatschappelijke risico's te verminderen. Daarnaast streeft het agentschap ernaar haar wettelijke taken zo efficiënt en effectief mogelijk uit te voeren. Dit doen we op basis van een sturingsfilosofie en toezichtmethodiek.

4.1 Sturingsfilosofie Toezicht

Toezicht vormt vanuit een gevoelde systeemverantwoordelijkheid een gezaghebbend oordeel over de goede werking van technische infrastructuren en over het vertrouwen in digitale infrastructuren. Toezicht intervenieert effectief langs de lijnen van modern toezicht waar nodig om de naleving te borgen. Toezicht is open en benaderbaar.

In onze sturingsfilosofie hanteren we de volgende uitgangspunten:

1. het toezicht is gebaseerd op informatiesturing en risicogerichtheid;
2. effectieve en efficiënte interventies waar nodig;
3. samenwerken met andere inspecties en overheidsorganisaties en dialoog met de omgeving om de effectiviteit van het toezicht te vergroten;
4. er is sprake van risico-aanvaarding;
5. er is een ontwikkelde signalerende en agenderende functie (reflectief toezicht);
6. er is een expliciete keuze om aan de voorkant van ontwikkelingen te komen.

De sturingsfilosofie verklaart het waarom achter de keuzes en functioneert als een filter voor het toezicht. Dat beperkt de toezichtlast voor de ondertoezichtgestelden en verhoogt het effect van ons toezicht. Met de sturingsfilosofie neemt Agentschap Telecom de principes van goed toezicht over, zoekt Toezicht de verbinding met de omgeving en kan zij met minimale last en maximaal resultaat toezicht houden.

4.2 Toezichtmethodiek

Agentschap Telecom opereert als toezichthouder in een breed toezichtdomein met gelimiteerde middelen. Om vanuit de geschetste ontwikkelingen op een efficiënte en effectieve manier de bijbehorende publieke belangen te beschermen en risico's te verminderen, is gekozen voor een methodiek voor prioritering van de toezichtactiviteiten en een ordening van de toezichtactiviteiten.

Prioriteren: informatie gestuurd en risicogericht

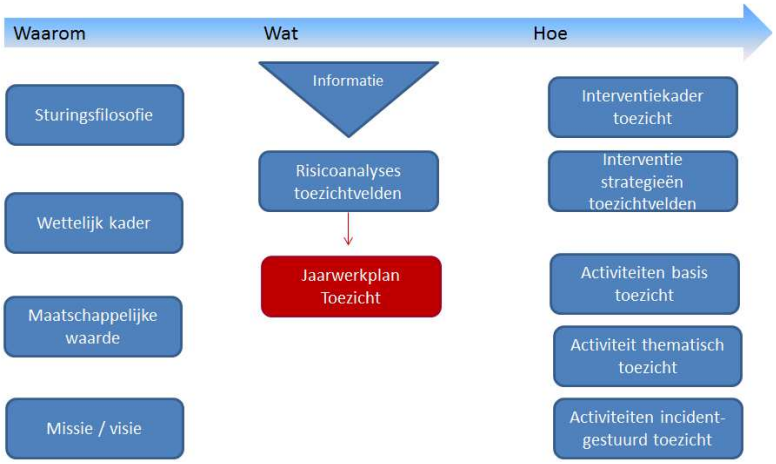
Enerzijds verwacht de maatschappij van het toezicht dat het alle risico's afvangt. Anderzijds wordt selectiviteit verwacht. Deze punten zijn strijdig met elkaar. De beperkte toezichtcapaciteit noopt tot keuzes en prioritering, waarbij het toezicht informatiegestuurd en risicogericht plaatsvindt. Juist bij selectiviteit kan sprake zijn van een restrisico bijvoorbeeld in de vorm van (ernstige) incidenten.

Toezicht kiest daarom bewust voor risicoaanvaarding, wetende dat niet alle risico's kunnen worden afgedekt. Uiteraard dienen we wel oog te blijven houden voor expliciete risico-aanvaarding en wordt in 2018 gemonitord en bewaakt of er veranderende signalen en sentimenten opkomen waardoor er

wel nadere invulling dient te worden gegeven aan expliciete risico-aanvaarding.

Om die reden werkt Toezicht met een flexibele programmering. Het basis toezicht maakt daarbij in voorkomend geval plaats voor incidentonderzoeken bij calamiteiten en voor thematische onderzoeken bij urgente maatschappelijke ontwikkelingen.

Voor het maken van keuzes hanteren wij een werkwijze op basis van risicoperceptie en risicosturing. Hieruit volgt een jaarlijks proces, gevoed door de beschikbare informatie(analyses). Per toezichtdomein of -thema wordt periodiek een analyse gemaakt van de relevante trends en ontwikkelingen, met oog voor maatschappelijke, politieke, technische en juridische ontwikkelingen. De uitkomst van dit proces bepaalt de prioritering van de uit te voeren toezichttaken. Dit uit zich in het volgende schema.



Indeling toezichtactiviteiten

De toezichtactiviteiten zijn onderverdeeld in drie categorieën, te weten:

- BASIS TOEZICHT

  Dit is het planbare reguliere (systematische) toezicht op de werkvelden (alle wettelijke taken), jaarlijks geprioriteerd volgens voornoemde systematiek. Het betreft veelal nalevingstoezicht waarbij op basis van informatiesturing gerichte steekproeven worden uitgevoerd. Bij patroonafwijkingen volgt veelal een thematisch onderzoek of een gerichte nalevingscampagne. Met het basistoezicht willen we een goede en storingsvrije werking van de technische infrastructuren bevorderen.

- THEMATISCH TOEZICHT

  Thematisch georiënteerde onderzoeken worden projectmatig opgepakt. Deze themaonderzoeken vloeien ook voort uit de prioritering waarbij het (potentiele) maatschappelijke belang of risico een grote rol speelt. De thematische onderzoeken leiden veelal tot signalering en/of agendering van een vraagstuk en is een belangrijk instrument om de reflectieve functie van toezicht vorm te geven. Hiermee dragen we bij om tijdig en continu te werken aan verbeteringen van onze infrastructuren om toekomstbestendig te worden en robuust te blijven.

- INCIDENTGESTUURD TOEZICHT

  Dit is het uitvoeren van onderzoeken n.a.v. incidenten met een hoge maatschappelijke relevantie (bijvoorbeeld een gasontploffing ten gevolge van een graafbeweging) of een actueel (telecom)vraagstuk (bijvoorbeeld de bereikbaarheid van 1-1-2 in een bepaalde omgeving). Dit zijn onvoorziene en niet geplande onderzoeken. Hiermee stimuleren we het systeemleren en het dragen we bij aan het oplossen en voorkomen van acute verstoringen in de infrastructuur.

4.3 Actieve samenwerking met andere rijksinspecties

Agentschap Telecom is actief lid van de Inspectieraad en neemt deel aan de gezamenlijke werkagenda. Onder meer door deelname aan de zogenaamde doe-coalities waarin de samenwerking rond een bepaald thema wordt georganiseerd.

Ook op concrete incidentonderzoeken wordt actief samengewerkt met andere inspecties. Voorbeelden uit het recente verleden zijn de incidentonderzoeken naar de bereikbaarheid van 1-1-2 en de diverse stroomstoringen samen met IJ&V en incidentonderzoeken naar gasexplosies samen met SodM.