Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Jaarplan Toezicht 2020

Agentschap Telecom

Voorwoord

De huidige mondiale digitaliseringsgolf biedt ook ons land ongekende en soms zelfs nog onbekende mogelijkheden. Digitalisering biedt kansrijke innovaties voor alle economische sectoren. Het stelt ons in staat verder te groeien, in bijna alle denkbare opzichten.
Nederland is in transitie.

De maatschappij omarmt alle mogelijkheden. De zorg innoveert, het onderwijs moderniseert en de logistiek automatiseert... Slimme apparaten nemen routinetaken van de mens over. En het internet of things nestelt zich in de huiskamer van de consument. De digitalisering dringt door tot in de haarvaten van onze samenleving. En maakt dat Nederland verder kan en vooruit komt.

Telecommunicatienetwerken en informatietechnologie vormen het onmisbare fundament onder dit proces. Gelukkig is die infrastructuur in Nederland van hoog niveau. Fysiek van uitstekende kwaliteit, alom beschikbaar en uiterst betrouwbaar. De vraag naar snelheid en capaciteit nemen al jaren toe. Evenals het gebruik. Dat geldt voor het individu, maar zeker ook op maatschappelijk niveau. De samenleving drijft op data. Een veilige digitale infrastructuur is een onmisbare voorwaarde voor welke economische branche of maatschappelijke sector dan ook.

Maar onmisbaar maakt afhankelijk. En afhankelijk maakt kwetsbaar. De landelijke storing van noodnummer 112 en de privacyschendingen door het hacken van beveiligingscamera's in 2019 tonen die kwetsbaarheid ook onomstotelijk aan. Ze voeden de maatschappelijke zorg voor ontwrichting op dit gebied.

Technologische ontwikkelingen schieten voortvarend wortel in het digitale domein. De potentiele impact van ontwikkelingen als kunstmatige intelligentie en blockchain is groot en de gevolgen kunnen zelfs disruptief zijn. Dat vereist modern toezicht. Adaptief, dynamisch, en met het vermogen om tijdig te detecteren en adequaat te reageren.

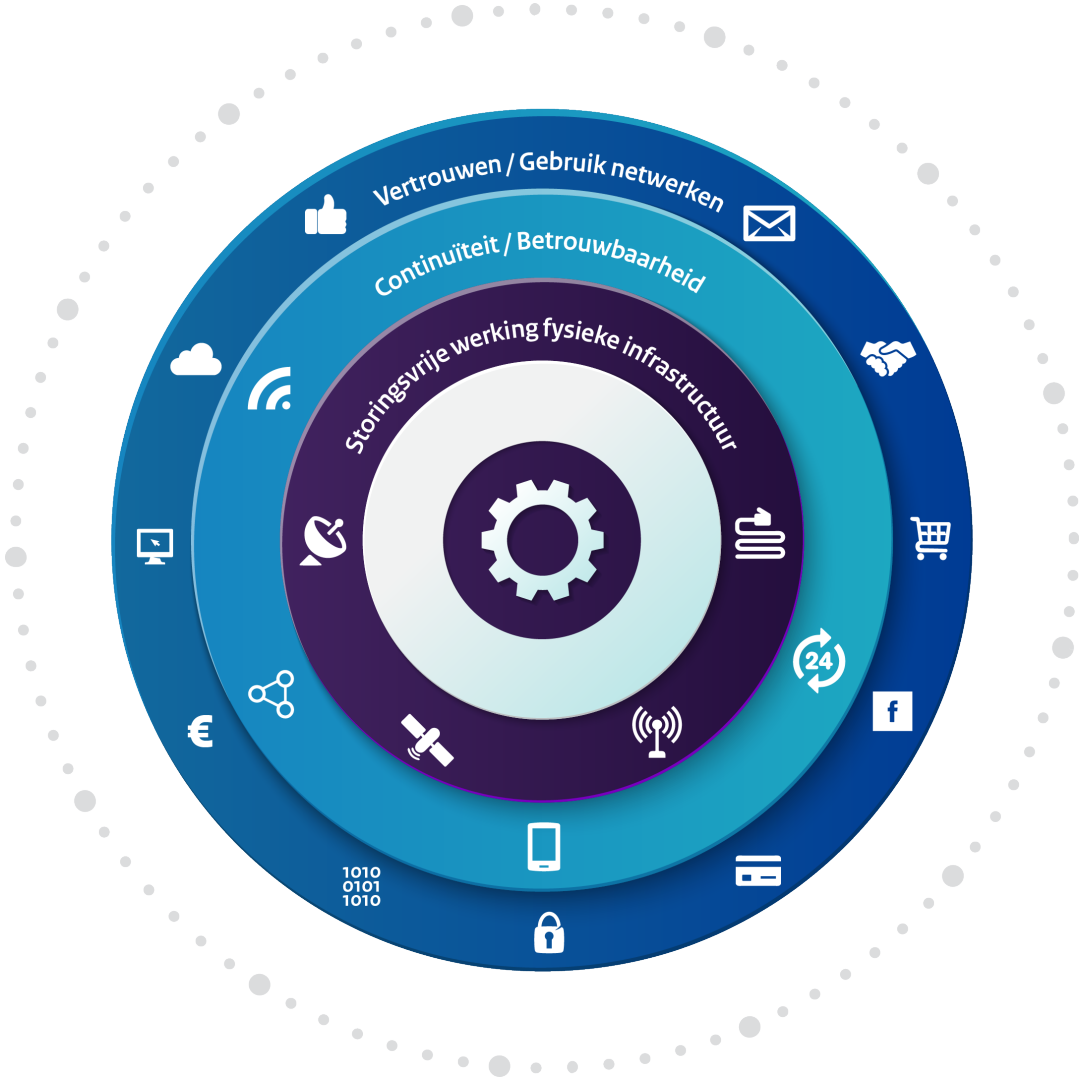
Nederland is in transitie. En Agentschap Telecom beweegt als toezichthouder vanzelfsprekend mee. Vanuit een klassieke taakopvatting naar kwaliteitstoezicht, van arbiter naar facilitator. Signalerend en agenderend.
En doortastend ingrijpend als de bescherming van het publieke belang dat vereist.

Agentschap Telecom, de autoriteit van de digitale infrastructuur en bewaker van het stelsel. Met de kwaliteit en betrouwbaarheid van vandaag. En met de integrale en dynamische oplossingen waar de dag van morgen om vraagt.

Angeline van Dijk
Directeur-hoofdinspecteur Agentschap Telecom

Inhoudsopgave

Hoofdstuk 1
Het digitale domein



Agentschap Telecom verstevigt de blijvende toegankelijkheid, beschikbaarheid en integriteit van technische infrastructuren, netwerken en diensten als de toezichthouder in het analoog en digitaal domein. Het domein dat voor iedere Nederlander dagelijks aan de orde is; in werk en privé.
Het toezicht van Agentschap Telecom is gericht op het beschermen van publieke belangen en de maatschappelijke vraagstukken die met de verregaande digitalisering invloed hebben op het gebruik van netwerken, diensten en het gebruik van apparatuur daarin.

Het digitaal domein omvat zowel de infrastructuur, de continue beschikbaarheid als het vertrouwen in het gebruik ervan. Integrale aandacht van de toezichthouder voor deze drie “ringen” (zie voorgaand figuur) borgt de integriteit in het digitaal domein en omvat daarmee tevens de deels nog analoge onderliggende infrastructuur. In het kader van het voorkomen van digitale ontwrichting is deze integrale aandacht een cruciale randvoorwaarde.

Binnen het digitaal domein richten de toezichtsvragen zich daarmee op beschikbaarheid, continuïteit, integriteit en vertrouwelijkheid van de informatie, netwerken, systemen en apparaten. Enkele voorbeelden en vragen die hierbij aan de orde zijn:

- Is de noodzakelijke verbinding om 112 te kunnen bellen gelegd? Kan het gesprek tijdig en juist plaatsvinden? Is het gesprek niet af te luisteren?
- Werkt mijn babyfoon, is deze storingsvrij en niet te hacken?
- Voldoet mijn zonnepaneel aan alle eisen en is de teruglevering mogelijk via het bestaande netwerk?
- Ben ik bereikbaar op mijn mobiel en kan ik zelf bellen vanuit dit natuurgebied?
- Heb ik ook echt 50 liter benzine getankt als de display dit vermeldt?
- Is mijn digitale handtekening veilig en betrouwbaar te gebruiken?
- Kan ik via deze website of marktplaats veilig aankopen doen?
- Heb ik nog wel stroom bij een hack op onze energievoorziening?
- Hartbewaking op afstand. Hoe veilig is dat?
- Wanneer kan ik 5G gebruiken op mijn smartphone?

Digitalisering maakt de samenleving echter ook op nieuwe manieren kwetsbaar voor verstoringen. Voorbeelden hiervan zijn de landelijke storing van het noodnummer 112 in de zomer van 2019 en privacyschendingen door het hacken van beveiligingscamera’s, eveneens in 2019. Dit voedt de zorg vanuit de maatschappij voor digitale ontwrichting.

Burgers, bedrijven en bestuursorganen moeten kunnen vertrouwen op een onafhankelijk toezichthouder die inzicht heeft in het speelveld, de juiste informatie over dit speelveld deelt en ingrijpt wanneer nodig. Agentschap Telecom stimuleert het vertrouwen in een aantal wezenlijke randvoorwaarden voor het functioneren van de maatschappij en de markt en draagt daarmee bij aan een gunstig ondernemingsklimaat en een veilige leefomgeving. Dit impliceert vrijheid maar betekent ook een grote verantwoordelijkheid voor de markt binnen het digitaal domein.

Onze missie is daarom:

"Agentschap Telecom staat voor de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken, zodat Nederland veilig verbonden is.”

Hoofdstuk 2
Ontwikkelingen in het digitaal domein

Telecommunicatie en IT zijn rand voorwaardelijk voor het functioneren van de economie en maatschappij. De digitalisering in dit domein gaat met een duizelingwekkende vaart. Zo snel dat de analoge alternatieven vaak niet meer bruikbaar zijn of niet meer aanwezig zijn[1]. Er is sprake van een grote verwevenheid van telecom en IT met de economie, veiligheidsvraagstukken en het dagelijkse maatschappelijke leven. Daarmee stijgt de zorg voor ontwrichting als het mis zou gaan in het digitaal domein[2].

De digitalisering in onze samenleving is de afgelopen jaren snel toegenomen en zal dat de komende jaren nog verder in hoog tempo doen. De invloed van de technologische ontwikkelingen en de maatschappelijke veranderingen bepalen ook de komende jaren sterk onze focus.

Nieuwe maatschappelijke vraagstukken dienen zich aan, waaronder de zorg voor digitale ontwrichting. De aard van deze vraagstukken is dynamisch: complex, onverwacht, snel en niet direct zichtbaar samenhangend met andere vraagstukken.

Dit vraagt om een dynamische benadering vanuit het toezicht. Door middel van systeemtoezicht gebaseerd op open normen. Dit alles in samenwerking met andere cruciale partners in de totale keten. Op die manier lossen we de problemen van vandaag op en proberen die van morgen te voorkomen.

De onderliggende oorzaak ligt onder andere in de snel veranderende techniek. Waar eerder in het analoge domein de functionaliteit van apparaten en systemen voornamelijk werd bepaald door de hardware, wordt in het digitaal domein de functionaliteit voornamelijk bepaald door de software. Een voorbeeld hiervan is de virtualisatie van telecomnetwerken. Mede daardoor verandert het digitaal domein in een hoog tempo. De dynamiek is groot op zowel techniek als toepassingen. Beiden laten zich niet hinderen door klassieke (fysieke) grenzen en indelingen.

In het analoge domein is vooral sprake van problemen of risico's die met gesloten normen beheersbaar gemaakt kunnen worden. De analoge techniek blijft belangrijk. Binnen de technische infrastructuur kunnen nog steeds problemen ontstaan die daarbinnen opgelost moeten worden. Verstoringen van draadloze communicatiesystemen door LED-installaties is hier een voorbeeld van.

[1] Grapperhaus, F. Ministerie van Justitie en Veiligheid, 12 juni 2019, Kamerbrief met beleidsreactie CSBN2019, P.1.
[2] Wetenschappelijke Raad voor het Regeringsbeleid (2019),Voorbereiden op digitale ontwrichting, wrr-Rapport 101, Den Haag:wrr.

In het digitaal domein zijn door de aard van de systemen de problemen en risico's dynamisch (denk aan software-updates, wijzigbare configuraties). Dit wordt versterkt door nieuwe technieken zoals AI en zelflerende algoritmen. Belangrijk is het vermogen om de bijbehorende problemen tijdig te detecteren en steeds mee te bewegen. In het digitaal domein waar vooral open normen gelden, denken wij dat samenwerking en systeemtoezicht daarom het meest effectief is. Daarbij is een toezichthouder die het domein kent en betrokken partijen tijdig hun verantwoordelijkheid laat nemen essentieel.

Vanuit de recente ontwikkelingen rond Internet of Things (IoT) en de cyberweerbaarheid van vitale infrastructuren komt nadrukkelijk naar voren dat het antwoord op de toenemende maatschappelijke zorg over digitale ontwrichting, naast adequaat toezicht, gezocht moet worden in de samenwerking met andere ketenpartners, zowel nationaal met o.a. NCSC als internationaal met Europese instituties zoals ENISA. De noodzakelijke toezichtsrol wordt daarmee in de bredere keten van overheidsverantwoordelijkheid geplaatst.
Vanuit deze achtergrond komen enkele relevante ontwikkelingen in beeld als focuspunten voor het werk van Agentschap Telecom voor het komend jaar.

- Als eerste zet de digitale transitie stevig door. Deze transitie vormt een belangrijke enabler voor de verdere groei in Nederland. Niet alleen vanuit economisch perspectief maar ook vanuit duurzaamheidsperspectief. De introductie van 5G en de verdere uitbreiding van het glasvezelnetwerk zijn belangrijke motoren achter de digitale transitie. Deze motoren brengen echter ook zorgpunten met zich mee over mogelijke negatieve effecten. 5G maakt snellere communicatie op meer plaatsen mogelijk en introduceert meer zichtbare basisstations in het straatbeeld. Voor de verdere verglazing moet de ondergrond in dorpen en steden vaker opengelegd worden. Voor ons betekent dit: focus op de nieuwe dekkings- en capaciteitsverplichting in gemeenten (paragraaf 3.1). En meer aandacht voor veilig en schadevrij graven en regie op de ondergrond, gezien de ondergrond het overgrote deel van de benodigde infrastructuur aan kabels en leidingen moet herbergen (paragraaf 3.1).

• De digitale transitie is tevens een randvoorwaarde voor een succesvolle energietransitie. Om decentraal energie op te wekken, te distribueren en te verrekenen is veel rekenkracht en datacommunicatie nodig. Maar ook andersom is er een grote afhankelijkheid. Om een duurzame, toekomstvaste en groenere samenleving te maken, moeten energie en digitale transitie hand in hand gaan. Voor ons betekent dit voor 2020 de volgende aandachtspunten : de mogelijke negatieve effecten beheersen, zoals storingen door zonnepanelen op vitale communicatiesystemen (paragraaf 3.3). En het scheppen van de juiste randvoorwaarden zoals betrouwbare energiemetingen te borgen met warmtemeters en slimme meters (paragraaf 3.3).

• Boven deze belangrijke ontwikkelingen hangt de zorg voor digitale ontwrichting. Een deel van het antwoord ligt in een robuuste, integere en veilige digitale infrastructuur. Met het toezicht op de Wet Beveiliging Netwerk- en Informatiesystemen, de elektronische identificatie en vertrouwensdiensten, elektronische toegangsdiensten en verscherpte zorgplicht voor Telecom Security legt Agentschap Telecom daar een stevige basis voor (paragraaf 3.2). Op samenwerking met andere (sectorale) toezichthouders, met partners in de cyberweerbaarheidsketen, zoals NCSC en DTC en internationale samenwerking op minimaal Europees niveau zetten we in 2020 stevig in (paragraaf 3.2).

Hoofdstuk 3
Programmering Toezicht 2020

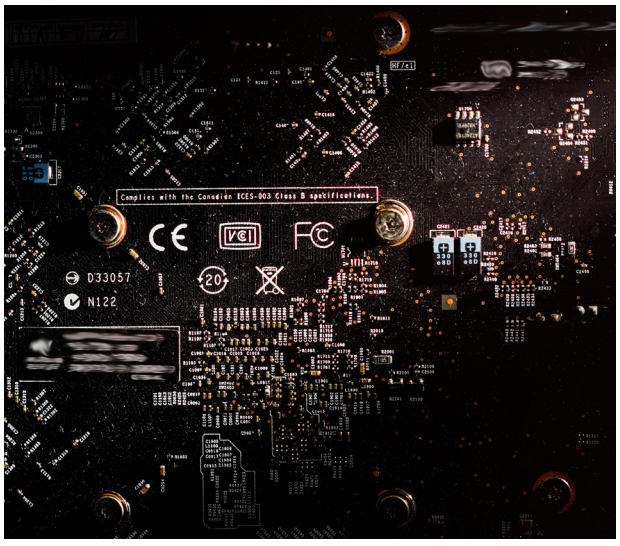
In lijn met de ontwikkelingen beschreven in hoofdstuk 2 en onze risicoschatting zet Agentschap Telecom voor 2020 in op de onderstaande programmering.

In deze programmering zijn de thema's digitale transitie en energietransitie leidend. Beschikbaarheid van nieuwe netwerken zoals 5G, regie op de ondergrond, storingsvrije en (digitaal) veilige werking van apparaten blijven onze aandacht vragen.

Daarnaast ligt het accent van ons toezicht op de verscherpte zorgplicht rond de continuïteit van telecom en IT-infrastructuren en het in kaart brengen van de afhankelijkheden in het digitaal domein. Zo kunnen wij in het stelsel met andere toezichthouders de zorg voor digitale ontwrichting voorzien van adequate antwoorden.

3.1 Toezicht op de beschikbaarheid van technische infrastructuren

Bij het toezicht op de technische infrastructuren gaat het om beschikbaarheid en storingsvrij gebruik van netwerken in gebruik bij de lucht- en scheepvaartsector, de OOV-diensten, bedrijfsnetwerken, satellietnetwerken en de openbare telecom- en omroepnetwerken. Het veilig en storingsvrij gebruik van elektrische en elektronische apparatuur is ook onderdeel van het toezicht op de technische infrastructuur. Burger en bedrijf moeten kunnen vertrouwen op de aanwezigheid en goede werking van de technische infrastructuur om dagelijks gebruik te kunnen maken van de aangeboden diensten.



Publiek belang	Risico	Toezichtdoel 2020	Speerpunten 2020
In Nederland willen we nu en in de toekomst een goede dekking en een optimale capaciteit van mobiele netwerken.	De invoering van sneller mobiel internet vertraagt. Onvoldoende mobiele dekking in gemeenten.	Een optimale transitie van de 2100 MHz band na heruitgifte om capaciteit van de banden beschikbaar te houden. Optimale naleving bij inwerkingtreding nieuwe dekkings- en capaciteitsverplichting in gemeenten (vanuit de 5G vergunningen).	Sturen op goede afspraken tussen vergunninghouders tijdens transitieproces in de 2100 MHz band. Pro actief toezicht op de verplichtingen (geldig vanaf 2022) om tijdig knelpunten te signaleren en een effectieve uitrol van 5G mogelijk te maken.
Bijdragen aan de continuïteit en veiligheid van bedrijfsprocessen in de industrie en MKB.	Verstoringen in cruciale communicatienetwerken.	Ongestoord frequentiegebruik van landmobiele vergunninghouders en naleving op het niveau conform vergunningen te krijgen.	Naleving bevorderen door interventies gericht op leveranciers en installateurs met nadruk op belangrijke maatschappelijke sectoren (o.a. BRZO, chemie, transport) en economisch belangrijke regio's.
Acceptabele kwaliteit van het radiolandschap.	Kwaliteit van de radio-ontvangst neemt af en/of storingen bij gebruik van vitale radiofrequenties.	Voorkomen en opheffen van verstoringen bij reguliere vergunninghouders en vitale frequentiegebruikers.	Voorlichtingscampagne over gebruik van goede apparatuur in DAB laag 6 voor lokale omroepen. Inrichting ketentoezicht bij de bestrijding illegaal FM frequentiegebruik om de effectieve aanpak te realiseren.
Leveringszekerheid van vitale diensten zoals energie, gas, water en telecom/ internet.	Onderbrekingen in vitale diensten omdat het aantal vermijdbare graafschades toeneemt.	Alle betrokkenen (opdrachtgever, netbeheerder en grondroerder) nemen hun verantwoordelijkheid in elke fase van het graafproces. De graafsector het aantal (vermijdbare) graafschades sterk te laten verminderen.	Toezicht op de naleving van de normen uit de CROW met focus op de belangrijkste opdrachtgevers. Samen met GPKL positioneren en faciliteren van de gemeente als regisseur van de ondergrond. Verscherpt toezicht op het tijdig aanleveren en verwerken van nieuwe informatie ligging kabels en leidingen.

3.2 Toezicht op continuïteit en integriteit van netwerken en diensten

Naast beschikbaarheid van technische infrastructuren als basis besteden wij in 2020 bijzondere aandacht aan de continuïteit en integriteit van netwerken en diensten. Netwerken dienen zo veel mogelijk beschermd te zijn tegen uitval als gevolg van externe factoren, zoals stroomuitval. Met name aan diensten zoals het 112-alarmnummer, dat ononderbroken toegankelijk dient te zijn, worden hoge eisen gesteld. Agentschap Telecom is tevens aangewezen als toezichthouder op de cyberweerbaarheid voor de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. Het doel van dat toezicht is de cyberweerbaarheid van onderhavige vitale infrastructuur te borgen. Daarnaast is Agentschap Telecom toezichthouder op elektronische identiteiten en vertrouwensdiensten en de informatieveiligheid van telecommunicatiediensten.

Publiek belang	Risico	Toezichtdoel 2020	Speerpunten 2020
Vitale diensten zoals burgeralarmering, bereikbaarheid alarmnummer 112 functioneren.	De burger kan 112 niet bereiken of wordt niet bereikt door NL-alert berichtgeving op drukbezochte locaties.	Continuïteit van dienstverlening NL-alert en 112.	Toezicht tijdens grote evenementen gericht op storingsvrij en continu gebruik van frequenties en vitale telecom.
Burgers en bedrijven kunnen ongestoord gebruik maken van telecom-diensten.	De continuïteit en/of integriteit van netwerken wordt bedreigd door externe factoren.	Aanbieders treffen adequate maatregelen om de continuïteit van hun netwerken en diensten te borgen.	Implementatie van de aangescherpte zorgplicht om de weerbaarheid te verhogen van telecomnetwerken (telecom security).
Beschermen van de continuïteit van diensten die van cruciaal belang zijn voor consumenten en bedrijven ter voorkoming van digitale ontwrichting.	Onvoldoende cyberweerbaarheid in de keten van vitale infrastructuren.	Aanbieders (essentiële diensten en digitaledienstverleners) treffen adequate maatregelen om de cyberweerbaarheid van vitale infrastructuren te borgen.	Uitvoeren van thematisch onderzoek om de afhankelijkheid, samenhang en overlap van een essentiële dienst en digitale dienstverlener te beoordelen.
		Digitale dienstverleners hebben een adequaat niveau van securitybewustzijn.	Door middel van voorlichting activatie van DSP's op het treffen van maatregelen voor cyberweerbaarheid.
		De impact van nieuwe ontwikkelingen op continuïteit van diensten wordt tijdig verwerkt in de toezichtstrategie.	Inventarisatie met collega toezichthouders op de betekenis van Artificial Intelligence, zowel horizontaal als binnen de specifieke sectoren.
	De kwaliteit van het certificeringsproces is onvoldoende om de cyberweerbaarheid te kunnen borgen.	Fabrikanten en dienstverleners treffen adequate maatregelen om de cyberweerbaarheid van hun producten, systemen en diensten te borgen.	Implementatie van het toezicht op cyberweerbaarheidscertificatieschema's en certificeringsbeoordelingsinstanties vanuit de Cyber Security Act.
Beschermen van de continuïteit en integriteit van IT-diensten op Europees niveau.	Door gebrek aan samenwerking onvoldoende waarborg op continuïteit en integriteit zijn van netwerken en diensten.	Hoog niveau van continuïteit en veiligheid van netwerken en diensten door samenwerking tussen Europese toezichthouder te stimuleren.	Invullen van leidende posities binnen ENISA , FESA en andere (EU) gremia versterven om door congruent Europees toezicht netwerken en diensten zo robuust mogelijk te maken.
Digitale elektronische transacties zijn betrouwbaar.	Nieuwe diensten die als handtekeningendienst gepresenteerd worden zijn niet betrouwbaar.	Burgers en bedrijven hebben inzicht in de rechtszekerheid van de verschillende vormen van elektronische handtekeningen.	Thematisch onderzoek naar de mate van rechtszekerheid die nieuwe innovatieve elektronische handtekeningdiensten bieden.
Informatievoorziening aan behoeftestellers is gegarandeerd.	Nieuwe technische ontwikkelingen maken bestaande opsporingsmiddelen minder goed bruikbaar.	Aftapbaarheid van diensten is goed geregeld. Specifiek in het geval van nieuwe innovatieve telecommunicatiediensten.	Verkenning aftapbaarheid toekomstige netwerken 5G. In samenwerking met J&V.

3.3 Toezicht op het gebruik en veiligheid van apparaten

Bij het toezicht op het gebruik en veiligheid van apparaten gaat het om eerlijke handel en het bevorderen van vertrouwen in het gebruik van apparatuur, zowel op het gebied van apparaat eigenschappen (werking, storingsgevoeligheid, elektromagnetische straling), als werking (software) als robuustheid tegen digitale bedreigingen.

Publiek belang	Risico	Toezichtdoel 2020	Speerpunten 2020
Een eerlijk speelveld voor fabrikanten, importeurs en distributeurs in Europa voor eerlijke handel. Daarbij moeten burgers en bedrijven erop kunnen vertrouwen dat apparatuur veilig is en goed werkt.	Storingen en onveilige situaties kunnen ontstaan door ondeugdelijke apparatuur.	Apparatuur voldoet aan de essentiële eisen uit de diverse EU- richtlijnen. Apparaten worden veilig gebruikt.	Implementatie van de LVD-taak en integratie met het bestaande toezicht op apparaten om veiligheid beter te borgen. Extra inzet op basistoezicht op RED en EMC om beter risico's te identificeren (in EU- verband). Toezicht op zonnepanelen en LED-installaties bij gebruik in de maritieme, industriële en kantooromgeving vanwege potentieel storende werking (signaal uit incidenten). Voorlichting over aanleg en normaal gebruik van componenten in iedere netgekoppelde zonnestroom installatie. Het bieden van handel-ingsperspectieven voor de gebruiker van vergunningvrije toepassingen voor de meest voorkomende storingsprob-lemen.
Meten en wegen van onder andere stroomverbruik, liters en kilo's bij in- en verkoop klopt: consument en bedrijf "krijgt waar voor zijn geld".	Onvoldoende kwaliteit geborgd bij nieuwe vormen van energielevering.	Betrokken partijen maken gebruik van betrouwbare meetinstrumenten (die belangrijk zijn voor de energietransitie).	Toezicht op gebruik van kwaliteitssystemen op het gebied van metrologie door partijen in de energiesector. Thematisch onderzoek naar het systeem rondom warmte-meters en laadpalen. Thematisch onderzoek naar de invloed van EM- veld op de werking van elektriciteitsmeters.

Een veilige en vlotte doorstroom van het scheepvaartverkeer.	Verslechterde communicatie op het water zorgt voor onveilige situaties en hindert een vlotte doorstroom.	Doelmatig gebruik en moderne maritieme apparatuur in lijn met de eisen.	Nu nog ontbrekende schakels binnen het stelsel van Automatic Identification System AIS (fabrikanten en installateurs) activeren en mobiliseren. Uitrollen campagne: “AIS? Een goed ID!” in ketensamenwerking met andere toezichthouders en sector.

Hoofdstuk 4
Onze visie op toezicht

Professioneel toezicht wordt binnen Agentschap Telecom gekenmerkt door verstand van zaken, in combinatie met verstand van toezicht. Toezicht opereert professioneel en betrouwbaar!

Publiek belang als uitgangspunt
Toezicht is er op gericht om de voor ons relevante publieke belangen te beschermen en maatschappelijke risico's op onze domeinen zo klein mogelijk te maken en te houden. Daartoe formuleren we de publieke belangen per domein expliciet als focuspunt. Om effectief te zijn willen we zoveel mogelijk aan de voorkant van maatschappelijke risico's komen.

Bewaker van het stelsel
Interne en externe samenwerking is essentieel. We zijn ons terdege bewust van de beperkte mogelijkheden die het toezicht in zijn algemeenheid heeft. Samen met onze collega's in de keten, beleid-uitvoering-toezicht vervullen we samen de rol van bewaker van het stelsel.

We zorgen voor tijdige detectie van relevante ontwikkelingen en een relevante kennisopbouw over het domein. De detectie doen we via interne en externe samenwerking en dialoog. We zijn daar transparant in om het debat met de stakeholders te stimuleren. Daarmee willen we tijdig inzicht krijgen en geven over de mogelijke maatschappelijke risico's en agenderen vanuit onze reflectieve functie.

Samenwerking nationaal en internationaal is de norm om dynamische vraagstukken aan te kunnen en de bijbehorende complexiteit te reduceren. Voorbeelden zijn:

- √ Op het gebied van continuïteit en integriteit van netwerken werken wij in internationaal verband samen met andere toezichthouders binnen het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), de NIS cooperation group en het Europese Forum voor toezichthoudende autoriteiten voor verleners van vertrouwensdiensten (FESA). Hiermee versterken wij onze preventieve en normerende functie voor kwaliteitssystemen en normeringen van de sectoren waarop wij toezicht houden.
- √ Op het gebied van veiligheid van apparatuur werken wij nationaal met onder andere de NVWA. Op internationaal niveau werken wij samen met andere autoriteiten naar eisen voor digitaal veilige apparatuur binnen de expertgroep van TCAM.
- √ Op nationaal niveau werken wij samen met Ministerie EZK en J&V en andere rijksorganisaties zoals het NCSC om problemen en risico's in het digitale stelsel vroegtijdig te signaleren.
- √ Wij werken samen met andere toezichthouders bij complexe incidentonderzoeken (zoals binnen de 112-keten).

Informatiegestuurd en risicogericht

Voor het maken van keuzes (zoals in dit jaarplan) hanteren wij een werkwijze op basis van risicoperceptie en sturing gevoed door de beschikbare informatie en analyses. We duiden periodiek de maatschappelijke risico's per (sub)domein. Door een werkwijze te hanteren waarbij de prioriteitstelling in het toezicht onderbouwd wordt door scherp de maatschappelijke risico's in de gaten te houden, trachten wij zo effectief mogelijk te zijn.

Wij richten het toezicht in volgens de lijnen van basistoezicht, thematisch toezicht en incidenttoezicht. De vertaling per domein is verschillend in verband met het type toezicht zoals nalevingstoezicht of kwaliteits-toezicht. In ons basistoezicht gebruiken wij zoveel als 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 effect het grootst is .

Op het gebied van toezicht en methodieken werken wij samen met andere toezichthouders binnen de Inspectieraad.

Onafhankelijk en met kennis van zaken

De samenleving moet kunnen vertrouwen op het onafhankelijk oordeel van ons als toezichthouder.

Vooraf betekent dit dat wij eigenstandig problemen en risico's binnen ons domein agenderen en signaleren. Gedegen onderzoek onderbouwt de tijdige signalering en agendering van maatschappelijke risico's. Daarnaast moeten wij in staat zijn om onafhankelijk informatie in te zamelen en daarover een eigen oordeel te kunnen vormen.

Technische kennis staat in onze organisatie hoog in het vaandel. Zo kunnen wij een goed en actueel beeld vormen van ons domein. Goed opgeleide en goed toegeruste inspecteurs en medewerkers vormen de kern van ons succes.

Effectieve en efficiënte interventies

Het pallet aan interventies is breed. Wij kijken naar het probleem en de meest passende interventie. In dit kader zijn wij aangesloten bij het Behavioural Insights Team van EZK. Aan de voorkant komen, betekent burgers en ondernemers bewust maken van risico's. Door handelingsperspectieven te bieden, te waarschuw-en, voorlichting en andere gedrag- beïnvloedende interventies willen wij de maatschappelijke risico's beperken. Waar nodig, bijvoorbeeld bij recidive of bij ongewenst gedrag dat risico's vergroot en veiligheid bedreigt, zetten wij sancties of boetes in.


5G
TELE2
MS-5445
RRU-6
LTE-800
Sector 3
Sector 3
ERICSSON