Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Op weg naar een veilige en weerbare digitale infrastructuur

Jaarplan Toezicht 2021

Agentschap Telecom

Op weg naar een veilige en weerbare digitale infrastructuur

Jaarplan Toezicht 2021

Agentschap Telecom

Voorwoord

Het jaar 2020 zal de boeken ingaan als het jaar van corona. Het jaar waarin we op anderhalve meter moesten leven, onze handen vaker wasten dan ooit en gewend raakten aan het dragen van mondkapjes. Het jaar ook waarin het werkende leven van velen drastisch veranderde. Van kantoor naar thuis, van bureau naar keukentafel en van collega's naar gezin of huisgenoten.

Dat was anders en wennen. Maar toch: het ging over het algemeen eigenlijk best goed. Onze netwerken bleken robuust genoeg om de piekbelasting als gevolg van het massale thuiswerken op te vangen. De digitale infrastructuur bleek een solide kurk waar onze economie en samenleving veilig op konden drijven.

Dat besef maakt dat we in een -deels misschien- verloren jaar toch ook heel belangrijke maatschappelijke winst hebben geboekt. We zijn meer dan ooit doordrongen van het belang van 'online' en digitalisering. We hebben aan den lijve ondervonden hoe het ons als individu en samenleving verder brengt. Zo gaf corona een enorme impuls aan de digitale transitie.

Want dat is wat er gaande is: Nederland en grote delen van de rest van de wereld verkeren in een digitale transitie. Dat is duidelijk zichtbaar en merkbaar. En zeker niet alleen op gebied van thuiswerken. In maatschappelijke sectoren als bijvoorbeeld energie, zorg, logistiek, landbouw, mobiliteit en duurzaamheid versmelt fysiek met digitaal. Bedrijfsprocessen en dienstverlening verlopen steeds meer geautomatiseerd. En daardoor optimaler, goedkoper en duurzamer dan voorheen mogelijk was.

Zo staat onze digitale infrastructuur allang niet meer op zichzelf. Was het vroeger nog slechts een middel om te kunnen bellen of internetten, tegenwoordig is het een onderdeel van een keten geworden. Faciliterend, voorwaardelijk en onmisbaar. Daardoor raakt ons werk als toezichthouder op de digitale infrastructuur ook andere economische sectoren. Alle economische sectoren.

Dat is een grote verantwoordelijkheid. Een verantwoordelijkheid die Agentschap Telecom wil pakken. Om kansen te grijpen voor Nederland, om Nederland verder te brengen. Want het welslagen van de digitale transitie is de enige route naar een gezonde, duurzame en welvarende toekomst.

Wij zien het als een gezamenlijke verantwoordelijkheid. Van de overheid, van het bedrijfsleven en ook van de burger. Over grenzen heen kijkend en intensief samenwerkend met andere toezichthouders en kennisinstituten op Europees niveau. Samen kunnen en zullen we Nederland veilig verbonden houden. Nu en in de intrigerende digitale toekomst die voor ons ligt.

Angeline van Dijk
Directeur-hoofdinspecteur Agentschap Telecom

Inhoudsopgave

1

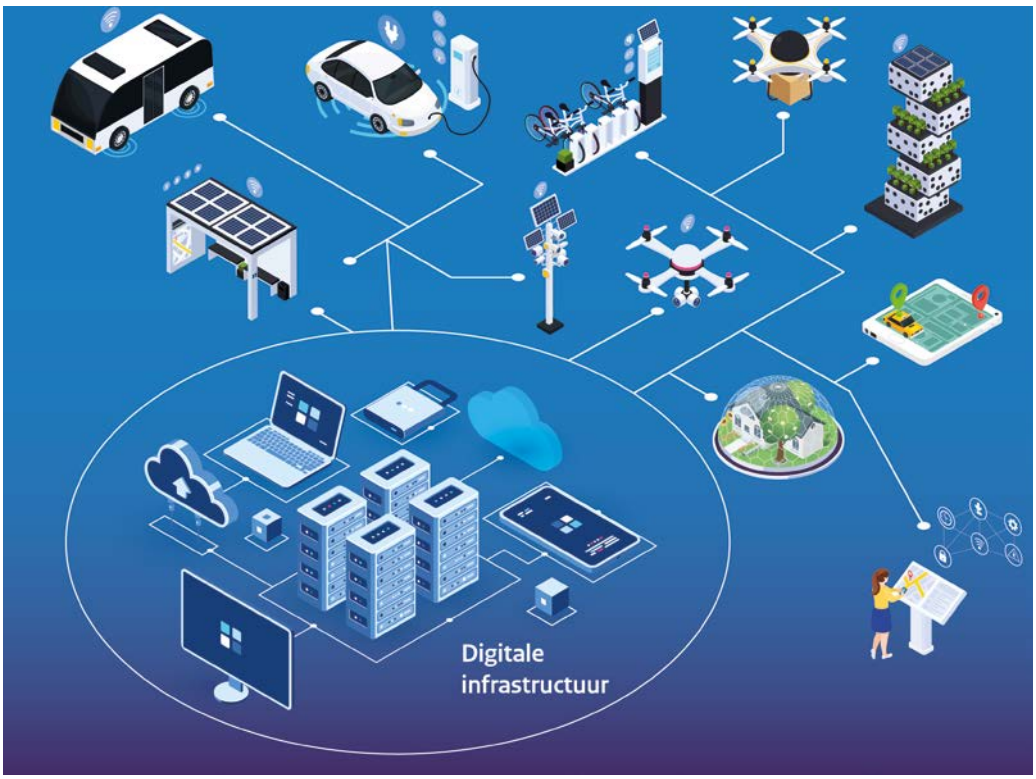
Trends en ontwikkelingen in het digitaal domein

1. Trends en ontwikkelingen in het digitaal domein

1.1 Digitalisering; een maatschappelijk belang

Digitalisering heeft een fundamentele impact op het leven in Nederland. Onze economie en ons sociaal welzijn steunen op digitale connectiviteit en digitale diensten.

De coronapandemie laat diepe sporen na in alle onderdelen van de (mondiale) samenleving. Bedrijven, zorginstellingen, scholen, overheden, burgers; alles en iedereen wordt direct of indirect geraakt door het virus of de gevolgen ervan. Maar de crisis biedt ook kansen. Digitalisering heeft door de uitzonderlijke omstandigheden een enorme boost gekregen en heeft haar maatschappelijke en economische mogelijkheden en meerwaarde nog maar eens uitdrukkelijk laten zien. Veel (vitale) processen kunnen doorgang vinden dankzij de inzet van de telecom- en internetsector. Er zijn creatieve, digitale oplossingen ontstaan voor werk, onderwijs en zorg en zij zijn op grote schaal succesvol uitgerold. De digitale infrastructuur verbindt consumenten, bedrijven en overheid en maakt de online samenleving mogelijk.



De borging van structurele aandacht van de Tweede Kamer in de vorm van de tijdelijke commissie Digitale toekomst, onderstreept de publieke belangen rondom digitalisering, zowel waar het gaat om de kansen als om de risico's.[1] Burgers, bedrijven en bestuursorganen moeten kunnen vertrouwen op een onafhankelijke toezichthouder. Agentschap Telecom **stimuleert het vertrouwen in de digitale infrastructuur** door zich te richten 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?

Onze traditionele onderwerpen zoals telecom, radiofrequenties, veilig graven en meetsystemen zijn geïntegreerd in ons toezicht op de beschikbaarheid, bereikbaarheid, veiligheid en betrouwbaarheid van de generieke (digitale) infrastructuur. Het digitaal domein omvat dus zowel de infrastructuur en de continue beschikbaarheid als het vertrouwen in het gebruik ervan. **Integrale aandacht** voor deze drie "ringen" (in bovenstaand figuur) borgt de integriteit van de generieke digitale infrastructuur en omvat daarmee tevens de deels analoge onderliggende infrastructuur.

1.2 Digitale infrastructuur; een complex en dynamisch stelsel

De keten van het digitaal domein als geheel is complexer en dynamischer geworden, waardoor het lastiger is te overzien waar kwetsbaarheden zijn. Door digitalisering groeien onderlinge afhankelijkheden en verbindingen tussen organisaties sterker. En dit gaat in een steeds sneller tempo.

Nieuwe doelgroepen komen in beeld. Vaste en mobiele operators, soft- en hardwareleveranciers, datahotels, platforms en digital service providers vormen gezamenlijk de digitale infrastructuur waar de samenleving op steunt. ICT en telecom versmelten in een complex stelsel van stakeholders. Zij dragen samen de verantwoordelijkheid voor het functioneren van de digitale infrastructuur waarop Agentschap Telecom integraal toezicht houdt.

Ook zien wij dat steeds meer elementen van logistieke en industriële processen onderdeel worden van de digitale infrastructuur. Anders gezegd: telecom en IT zijn geen verschijnselen op de achtergrond maar integreren in alle deelfacetten en -sectoren van de samenleving. In plaats van te kijken naar individuele organisaties en (naar een op het oog) geïsoleerde casuïstiek, is een brede en integrale blik nodig over factoren, sectoren en actoren heen.

[1] De tijdelijke commissie Digitale toekomst (TCDT) van de Tweede Kamer heeft onderzocht hoe het parlement meer grip op digitalisering kan krijgen. Er zijn diverse aanbevelingen gedaan, waarvan één was gericht op passende regulering en toezicht. Onlangs is er een motie aangenomen over het instellen van een vaste commissie voor digitale zaken. De commissie wordt na de aankomende verkiezingen in de Tweede Kamer geïnstalleerd.

Agentschap Telecom heeft als toezichthouder op de digitale infrastructuur de unieke positie, rol en expertise waarmee we de ketens weten te ontrafelen en tegelijkertijd integraal te overzien, alsook te bepalen op welk specifiek (sub)onderdeel (extra) inzet nodig is om ongewenste risico's op systeemfalen vroegtijdig te voorkomen of op te lossen.

1.3 Digitale infrastructuur; vergroten van de weerbaarheid en veiligheid

We hebben het in Nederland goed voor elkaar als het op digitalisering aankomt. Toch worden ook maatschappelijke zorgen over risico's en gevolgen van digitalisering prominenter. Bijvoorbeeld als het gaat om de digitale weerbaarheid (cyberweerbaarheid) en security, bij alle (vitale) processen en in ons dagelijks leven. En ook over de veiligheid van apparaten en netwerken.

Het Rathenau Instituut verwoordt de cyberweerbaarheid treffend[2]:
"We ontdekten dat cyberweerbaarheid is als het menselijk immuunsysteem. Dat is niet in staat alle aanvallen buiten de deur te houden. Het immuunsysteem rekent met indringers en interne incidenten af of probeert ze onder de duim te houden. Wie gezond is en preventieve maatregelen neemt, slaagt daar beter en langer in."

Onvoldoende weerbaarheid in het digitaal domein en onvoldoende beheersing van risico's schaden het *vertrouwen in de digitale infrastructuur*, terwijl dat vertrouwen juist fundamenteel is voor het economisch en maatschappelijk welbevinden in en van Nederland. Met haar toezicht draagt Agentschap Telecom bij aan dat vertrouwen.

Het belang en de urgentie daarvan volgt ook uit de recente update van *de Nederlandse Digitaliseringsstrategie (NDS): "Doordat digitalisering steeds meer en breder toegepast wordt, wordt digitale weerbaarheid in een groeiend aantal situaties een randvoorwaarde voor de continuïteit van digitaal aangestuurde processen.*
Digitale weerbaarheid is daarnaast een noodzakelijke randvoorwaarde voor het behoud van vertrouwen van burgers en bedrijven in digitalisering: iedereen moet kunnen vertrouwen op de veiligheid van digitale producten en diensten."

De NDS meldt dat het Cyber Security Beeld Nederland 2020, net als in 2019, een zorgwekkend dreigingsbeeld schetst en aangeeft dat er extra stappen nodig zijn voor digitale weerbaarheid, onder meer door het versterken van toezicht en interventiemogelijkheden.

Extra stappen digitale weerbaarheid
De eerder door Agentschap Telecom gesignaleerde ontwikkelingen en speerpunten ten aanzien van ***continuïteit, weerbaarheid en security*** zijn onverminderd relevant gebleken. Agentschap Telecom zal haar focus op die thema's voortzetten.

Agentschap Telecom houdt ook in 2021 toezicht op de aangescherpte zorgplicht voor security, waaronder de nieuwe regels voor het gebruik van specifieke apparatuur in telecomnetwerken. Er wordt onderzoek gedaan naar het volwassenheidsniveau van aanbieders en er vinden thematische inspecties plaats die gericht zijn op netwerk- en informatiesystemen (hoofdstuk 2.2). Het toezicht op cyberbeveiligingscertificeringsregelingen en conformiteitsbeoordelingsinstanties vanuit de Cyber Security Act wordt in 2021 verder geïmplementeerd zodat deze nieuwe taak op adequate wijze kan worden ingevuld.

[2] Rathenau Instituut (2020). Cyberweerbaar met nieuwe technologie – Kans en noodzaak van digitale innovatie. Den Haag (auteurs: Boheemen, P. van, G. Munnichs, L. Kool, G. Diercks, J. Hamer & A. Vos)

Om de weerbaarheid van telecomnetwerken tegen zogeheten ‘supply chain attacks’[3] te verhogen, heeft het kabinet aanvullende maatregelen getroffen. Op 5 december 2019 is het Besluit veiligheid en integriteit telecommunicatie gepubliceerd. Op basis van dat besluit worden extra hoge eisen gesteld aan leveranciers van diensten en producten in de kritieke onderdelen in het telecomnetwerk. Daarnaast worden aan aanbieders van mobiele netwerken technische en organisatorische beveiligingsmaatregelen opgelegd die in een ministeriële regeling worden vastgelegd. Agentschap Telecom gaat na de eerste fase, waarin risico’s in beeld zijn gebracht en wetgeving is opgesteld, nu toezicht houden op de invulling en uitwerking van deze maatregelen. De maatregelen die genomen zijn, vragen een forse inspanning van de telecomindustrie en de implementatie ervan vergt enkele jaren.

De focus van het toezicht op apparaten wordt uitgebreid met cyberweerbaarheid. Het doel van deze uitbreiding is om de markt aan de voorkant te beïnvloeden en een beweging richting “secure by design” te creëren.
Daarmee worden cyberweerbaarheid- en securityrisico’s verkleind en het vertrouwen van gebruikers in de veiligheid van apparaten vergroot.

[3] Een cyberaanval die een organisatie probeert te beschadigen door zich te richten op minder veilige elementen in het supply netwerk. Een aanval op de toelevering kan voorkomen in elke bedrijfstak, van de financiële sector, de olie-industrie tot de publieke sector.

Extra stappen veiligheid van apparaten

De maatschappelijke zorg over de veldsterkteniveaus van de nieuwe 5G-apparatuur is het afgelopen jaar sterk naar voren gekomen. Ook 5G-apparatuur moet voldoen aan de Europese eisen die gesteld zijn aan onder andere het uitzenden van elektromagnetische straling (ICNIRP-limieten). Agentschap Telecom intensiveert de metingen in het veld om te controleren of de niveaus beneden deze limieten blijven en om op te treden indien dit onverhoopt niet zo is. Dit is één van de activiteiten om de uitrol van 5G op een verantwoorde manier te laten verlopen.

Samenwerking nationaal en internationaal

Om digitale weerbaarheid in de samenleving te vergroten, moet ook binnen de overheid worden samengewerkt om tot een maximale bijdrage te komen. Ieder onderdeel van de overheid vanuit zijn eigen rol. Onder andere opsporing, informatieknooppunten en toezicht.

Agentschap Telecom zet daarom in op het verder versterken van de samenwerking, kennisdeling en informatie-uitwisseling tussen het Nationaal Cyber Security Centrum (NCSC), vitale sectoren en sectorale toezichthouders over bijvoorbeeld de betekenis van Artificial Intelligence (AI) en nieuwe digitale toepassingen.

In het kader van Europese samenwerking bekleedt Agentschap Telecom leidende posities in diverse Europese overlegstructuren met toezichthouders van andere lidstaten.

Signaleren en agenderen nieuwe (disruptieve) technieken

De ontwikkelingen rondom digitalisering en toepassingen zoals AI gaan door. Agentschap Telecom heeft een analyse laten uitvoeren naar het (toekomstige) gebruik van AI in de telecomsector en de kansen en risico's die daaraan verbonden zijn. Uit het onderzoek van Dialogic blijkt dat het gebruik van **AI** sterk zal toenemen en dat die toename nog versneld wordt met de komst van **5G**. Het onderzoeksrapport geeft richting aan de invulling van het toezicht op AI, nu en in de toekomst. Allereerst voor de telecomsector, maar mogelijk daarna ook voor andere sectoren waarin AI steeds meer wordt toegepast, zoals transport & logistiek, energie en zorg.

Als toezichthouder op de generieke digitale infrastructuur signaleert en duidt Agentschap Telecom nieuwe en disruptieve technieken. We willen weten wat **het effect van deze technieken** is op onder meer de betrouwbaarheid van vertrouwensdiensten, security en weerbaarheid.

In 2021 voeren we thematische onderzoeken uit naar de inzet van onder andere AI bij persoonsidentificatie, digitale transacties en het gebruik van 'alternatieve' vertrouwensdiensten die niet de vereiste betrouwbaarheid bieden. Ook het vervolg van het thematisch onderzoek naar metrologie- en cyberweerbaarheidsaspecten van laadpalen is een voorbeeld van de signalerende rol van Agentschap Telecom ten aanzien van belangrijke ontwikkelingen in de (digitale) infrastructuur.

De uitkomsten van deze thematische onderzoeken gebruiken we om eventuele vervolgacties te bepalen of om nieuwe kansen en risico's te adresseren. Met onze onderzoeken vormen we een beeld of met nieuwe digitale technische toepassingen nog steeds de bestaande regels nageleefd worden. Blijkt dat bestaande regels niet toereikend zijn, dan signaleren wij dat bij de wetgever, zodat deze daar bij wetsvoorstellen rekening mee kan houden.

Ook op die manier dragen we vanuit onze rol als toezichthouder op de digitale infrastructuur bij aan het maatschappelijk en economisch welbevinden van Nederland.

2

Programmering Toezicht 2021

2 Programmering Toezicht 2021

In lijn met de trends en ontwikkelingen en onze risicoschatting, zet Agentschap Telecom voor 2021 in op de onderstaande programmering van haar toezicht[4]:

In deze programmering staan een aantal maatschappelijke relevante thema's centraal.
Ons toezicht draagt hieraan bij en richt zich op de beschikbaarheid, weerbaarheid en security van technische infrastructuren en het vertrouwen in het gebruik en veiligheid van apparaten.

2.1 Centrale thema's in ons toezicht

Uitrol 5G | Duiding nieuwe technieken (AI) | Veilige apparaten | Weerbare vitale infrastructuren

De focus in onze programmering ligt in 2021 onder andere op de **uitrol van 5G**. De nieuwe vergunningen moeten met stevige eisen in gebruik genomen worden, zodat zoveel mogelijk mensen en bedrijven kunnen beschikken over veilige en snelle mobiele dataverbindingen. In telecommunicatie- en IT-systemen worden de nieuwste technieken gebruikt, zoals **Artificial Intelligence**. We hebben in 2020 een onderzoek laten uitvoeren wat dit voor ons toezicht betekent en we starten dit jaar met de invoering van de aanbevelingen. Zodat Nederland veilig verbonden blijft!

We intensiveren ook ons toezicht op apparaten. Dat is elementair voor het vertrouwen in de digitalisering die cruciaal is voor onze economische positie. **Apparaten** die voor ons dagelijks functioneren belangrijk zijn, zoals smartphones en IoT-apparatuur, moeten veilig te gebruiken zijn. Daarom kijken we in ons toezicht integraal naar deze veiligheidsaspecten. Niet alleen storingsvrij werken is belangrijk, maar ook digitaal veilig en elektrisch veilig. En... werkend binnen de toegestane veldsterktelimieten.

[4] We dienen echter rekening te houden met een scenario dat aanhoudende effecten van de coronapandemie een complicerende rol kunnen spelen bij de feitelijke uitvoering van de toezichttaken uit de programmering.

In de achterliggende telecommunicatie en energie-infrastructuur is de **cyberweerbaarheid** voor ons topprioriteit. Waarbij we oog hebben voor de steeds verdergaande **ketenafhankelijkheden tussen deze infrastructuren**.

2.2 Toezicht op beschikbare technische infrastructuren

Is de infrastructuur aangelegd en verbonden?

Bij het toezicht op de technische infrastructuren gaat het om beschikbaarheid en storingsvrij gebruik van netwerken die door de lucht- en scheepvaartsector, de OOV-diensten, bedrijfsnetwerken, satellietnetwerken en de openbare telecom- en omroepnetwerken worden gebruikt. Voor hun maatschappelijke en economische belangen moeten burgers en bedrijven kunnen vertrouwen op de aanwezigheid en goede werking van de (digitale) technische infrastructuur.

Publiek Belang
Goede dekking en een optimale capaciteit van mobiele netwerken.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Vertraging van de invoering van sneller mobiel internet.	Een optimale transitie van de 2100 MHz band na heruitgifte om de beschikbaarheid te borgen.	Toezicht op het ordelijk verloop van het transitieproces in de 2100 MHz band waarbij vergunninghouders omschakelen van oude naar nieuwe frequenties voor sneller mobiel internet. Uitrol 5G
Onvoldoende mobiele dekking in gemeenten.	Optimale naleving bij inwerkingtreding nieuwe dekkings- en capaciteitsverplichting in gemeenten.	Proactief toezicht op de verplichtingen (geldig vanaf 2022) om tijdig potentiële knelpunten te signaleren en een effectieve uitrol van 5G mogelijk te maken. Uitrol 5G

Publiek Belang
Continuïteit en veiligheid van bedrijfsprocessen bij het gebruik van draadloze communicatie in de industrie en MKB.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Verstoringen in cruciale industriële communicatienetwerken.	Ongestoord frequentiegebruik van vergunninghouders in de landmobiele sector (o.a. BRZO-bedrijven).	Verdere intensivering van het toezicht op de samenhang in de keten inclusief leveranciers, installateurs en vergunninghouders. Focus op het gebruik in economisch belangrijke regio's. Weerbare vitale infrastructuren

Publiek Belang
Acceptabele kwaliteit van het radiolandschap.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Technische kwaliteit van de radio-uitzendingen neemt af en/of storingen bij gebruik van vitale radiofrequenties.	Voorkomen en opheffen van verstoringen bij reguliere vergunninghouders en vitale frequentiegebruikers.	Gerichte inspecties op de naleving van technische voorschriften door nieuwkomers. Inrichting ketentoezicht met externe partners zoals politie, OM, t.b.v. door illegale activiteiten de zwaarst getroffen FM-radionetten.

Publiek Belang
Beschikbare netwerken voor vitale overheden.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Overheden kunnen bij het uitoefenen van hun taken niet ongestoord communiceren.	Voorkomen en opheffen van verstoringen bij vitale frequentiegebruikers.	Monitoring en onderzoek van de spectrumbanden die gebruikt worden door betreffende vitale frequentie-gebruikers met name gericht op (potentiële) intruders. Weerbare vitale infrastructuren
Overheden maken (nagenoeg) geen gebruik van schaars spectrum.	Inzicht in het gebruik van het spectrum door overheden. Hiermee voorkomen van onnodig toewijzen van schaars spectrum aan overheden.	Monitoring en onderzoek feitelijk frequentie-gebruik op luchthavens, bij evenementen en tijdens oefeningen.

Publiek Belang
Leveringszekerheid van vitale diensten zoals energie, gas, water en telecom/ internet.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
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.	Gerichte inspecties op de partijen in de graafketen om te toetsen op de vastgestelde normen (CROW500). Met focus op de belangrijkste opdrachtgevers. Onderzoek naar de *best practices* om gemeenten in hun kracht te zetten in hun rol als regisseur van de ondergrond. In samenwerking met het Gemeentelijk Platform Kabels en Leidingen (GPKL). Het ontwikkelen van een signalering-systeem om datagedreven vast te kunnen stellen hoe op enig moment het naleef-gedrag van de diverse actoren in de graafketen is.
	De graafsector het aantal (vermijdbare) graafschades sterk te laten verminderen.	Verscherpt toezicht op het aanwezig hebben en hanteren van werkinstructies door de grondroerders. Uitrol 5G Weerbare vitale infrastructuren Verscherpt toezicht op het tijdig aanleveren en verwerken van nieuwe informatie door netbeheerders over de ligging van kabels en leidingen.

2.3 Toezicht op security en weerbaarheid van netwerken en diensten

Zijn de netwerken en diensten continu bereikbaar en veilig?

Naast beschikbaarheid van technische infrastructuren wordt in 2021 het toezicht op de continuïteit en integriteit van netwerken en diensten voortgezet. Gelet op de gesignaleerde ontwikkelingen, neemt het belang van ons toezicht alleen maar toe. Netwerken dienen zo adequaat mogelijk beschermd te zijn tegen uitval als gevolg van externe factoren, waaronder onbedoeld door menselijke fouten dan wel bedoeld zoals door een hacker. Het kan daarbij bijvoorbeeld gaan om het noodnummer 112, maar ook om de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. Agentschap Telecom ziet toe op de borging van cyberweerbaarheid van de vitale infrastructuur door de ondertoezichtgestelden. Daarnaast houdt Agentschap Telecom toezicht op elektronische identiteiten en vertrouwensdiensten en de informatieveiligheid van telecommunicatiediensten.

Publiek Belang
Vitale diensten zoals burgeralarmering, bereikbaarheid alarmnummer 112 functioneren.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
De burger kan 112 niet bereiken of wordt niet bereikt door NL-alert berichtgeving op druk-bezochte locaties.	Continuïteit van dienstverlening NL-alert en 112.	Toezicht tijdens grote evenementen gericht op storingsvrij en continu gebruik van frequenties en vitale telecom. Weerbare vitale infrastructuren

Publiek Belang
Burgers en bedrijven kunnen ongestoord gebruik maken van telecomdiensten.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
De continuïteit en/of integriteit van netwerken wordt bedreigd door het gebruik van ongewenste systeemcomponenten.	Aanbieders treffen adequate maatregelen om de continuïteit van hun netwerken en diensten te borgen.	Toezicht op de aangescherpte zorgplicht i.h.k.v. telecomsecurity, waaronder de aangescherpte technische maatregelen voor het gebruik van specifieke apparatuur in telecomnetwerken. Uitrol 5G Weerbare vitale infrastructuren

Publiek Belang
Beschermen van de continuïteit van diensten die van cruciaal belang zijn voor consumenten en bedrijven ter voorkoming van digitale ontwrichting.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Onvoldoende cyberweer-baarheid in de keten van vitale infrastructuren.	Aanbieders (essentiële diensten en digitaledienstverleners) treffen adequate maatregelen, o.a. ten aanzien van aanvalsvectoren – en methoden, supply-chain en Business continuity management (BCM), met als doel om de cyberweerbaarheid van vitale infra-structuren te borgen.	Risicogerichte thematische inspecties op de kwaliteit van de gebruikte netwerk- en informatiesystemen van vitale aanbieders. Weerbare vitale infrastructuren
	Aanbieders (essentiële diensten en digitale-dienstverleners) hebben een adequaat niveau van security bewustzijn.	Inspecties naar het volwassenheids-niveau van cyberweerbaarheid bij aanbieders van essentiële diensten. Weerbare vitale infrastructuren

Publiek Belang
Beschermen van de continuïteit van diensten die van cruciaal belang zijn voor consumenten en bedrijven ter voorkoming van digitale ontwrichting.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
	Volgen en duiden van disruptieve technieken t.a.v. security en weerbaarheid.	Versterken van de samenwerking en kennisdeling met collega toezichthouders over de betekenis van Artificial Intelligence (AI). Duiden gebruik van AI bij digitale persoonsidentificatie, digitale transacties en het gebruik van "alternatieve" vertrouwensdiensten. Duiding nieuwe technieken (AI)
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.	Inrichting van het toezicht op cyberbeveiligingscertificeringsregelingen en conformiteitsbeoordelingsinstanties vanuit de Cyber Security Act. Weerbare vitale infrastructuren Veilige apparaten

Publiek Belang
Beschermen van de continuïteit en integriteit van IT-diensten op Europees niveau.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Door gebrek aan Europese samenwerking onvoldoende waarborg op continuïteit en integriteit van netwerken en diensten.	Hoog niveau van continuïteit en veiligheid van netwerken en diensten door samenwerking tussen Europese toezichthouders te stimuleren.	Continueren van leidende posities binnen ENISA , FESA, DSP workinggroup en andere (EU) gremia, alsmede samenwerking verstevigen om door congruent Europees toezicht, netwerken en diensten zo robuust mogelijk te maken. Duiding nieuwe technieken (AI) Weerbare vitale infrastructuren

2.4 Toezicht op veilige apparaten

Werken de apparaten en instrumenten goed en veilig?

Bij het toezicht op het gebruik en de veiligheid van apparaten gaat het om eerlijke handel en het bevorderen van vertrouwen in het veilig gebruik van apparatuur die goed werkt. Daarbij gaat het om apparaateigenschappen (werking, storingsgevoeligheid, elektromagnetische straling, elektrische veiligheid), om de veilige werking (software) en robuustheid tegen digitale bedreigingen. Apparatuur is daardoor veilig te gebruiken, betrouwbaar in het gebruik en stoort niet.

Publiek Belang
Een eerlijk speelveld voor fabrikanten, importeurs en distributeurs in Europa voor gelijke handel.
Burgers en bedrijven kunnen erop vertrouwen dat apparatuur en meetinstrumenten veilig zijn en goed werken.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Storingen en onveilige situaties kunnen ontstaan door ondeugdelijke apparatuur.	Betrokken partijen maken gebruik van betrouwbare apparaten en meetinstrumenten die voldoen aan de wettelijke eisen.	Onderzoek naar de (elektrische) veiligheid van apparaten om te signaleren welke productgroepen het grootste maatschappelijke risico vormen. **Veilige apparaten** Intensivering EMV-metingen bij de uitrol van 5G-netwerken. **Veilige apparaten** **Uitrol 5G** Ontwerp en bouw IoT testlab. **Veilige apparaten** **Uitrol 5G** Afspraken met grotere e-commerce bedrijven over het weren van producten die niet voldoen aan Europese regelgeving. Het bieden van handelingsperspectieven voor de gebruiker van vergunningvrije toepassingen voor de meest voorkomende storingsproblemen.

Publiek Belang
Een eerlijk speelveld voor fabrikanten, importeurs en distributeurs in Europa voor gelijke handel.
Burgers en bedrijven kunnen erop vertrouwen dat apparatuur en meetinstrumenten veilig zijn en goed werken.

Risico 's	Toezichtdoel 2021	Speerpunten 2021
Meetinstrumenten die worden gebruikt bij handelstransacties meten niet goed.		Toezicht op gebruik van kwaliteitssystemen door marktpartijen op het gebied van metrologie. Thematisch onderzoek naar metrologische cyberweerbaarheidsaspecten van laadpalen. **Weerbare vitale infrastructuren** **Veilige apparaten**

3

De principes van ons toezicht

3 De principes van ons toezicht

We houden toezicht door vroegtijdig aan de voorkant van de problematiek in het digitaal domein te komen, door te weten wat er speelt en adequaat en responsief te interveniëren. Daarmee dragen we bij aan het tijdig oplossen of voorkomen van systeemfalen en aan een cyberweerbare, betrouwbare en integere digitale infrastructuur.

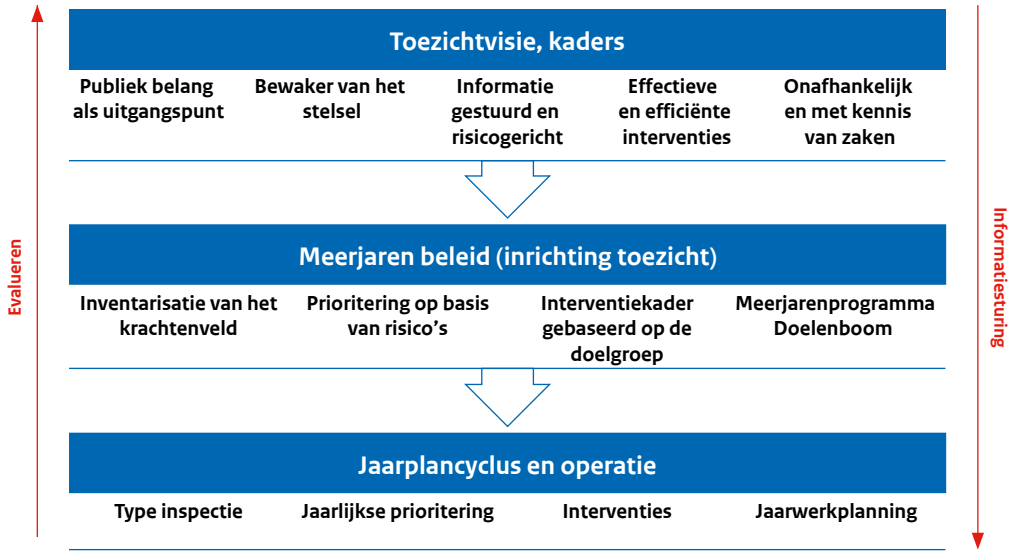
Publiek belang als uitgangspunt

Ons toezicht is erop gericht om de relevante **publieke belangen** binnen onze werkvelden te beschermen en maatschappelijke risico's zo klein mogelijk te maken en te houden, en zodoende duurzame economische ontwikkeling te ondersteunen. De publieke belangen per domein vormen expliciet het focuspunt van ons toezicht. Daarbij kijken we verder dan de regels, wij kijken ook naar hetgeen de maatschappij nodig heeft en waar we met ons toezicht maatschappelijke waarde kunnen creëren.

Om effectief en gezaghebbend te zijn, willen we zoveel mogelijk aan de voorkant van maatschappelijke risico's komen. Dit omvat een responsieve houding en benadering, waarin we signaleren, voorspellen, adviseren, maar zo nodig ook arbitreren.

Bouwstenen van ons toezicht

Inspectie, monitoring & analyse alsmede de toezichtvisie en strategische kaders komen samen in het bouwwerk toezicht, dat door ons is ontwikkeld om goed te kunnen sturen op het reduceren van **maatschappelijke risico's**.



Binnen deze structuur bepalen we welke vorm van toezicht aansluit bij de doelen in termen van beleid en toezicht. We voeren domein- en clustergerichte omgevings- en risicoanalyses uit, om hierna te bepalen welke overtreding of risico prioriteit heeft. Hiervoor investeren we continu in het optimaliseren van onze toezichtmethodieken en het gebruik van data als grondstof voor onze aanpak in informatiegestuurd en risicogericht toezicht.

Onze interventies zijn erop gericht om op een effectieve manier gewenst gedrag bij de doelgroepen te bereiken. Maar zij zijn breder dan dat: de vragen van deze tijd vergen meer en meer een voorbereidende rol van het toezicht. Juist in deze pre-fase van het toezicht zijn onze interventies gericht op het verbinden van marktpartijen, het bieden van effectieve oplossingsrichtingen, het initiëren van nieuw beleid en bijvoorbeeld het bieden van handelingsperspectieven voor burgers en het bedrijfsleven.

Doelregelgeving en inrichting van ons toezicht

Zoals in eerdere hoofdstukken is aangegeven, is ons toezicht de afgelopen jaren gegroeid naar een breder taakveld met **nieuwe doelgroepen en ketenpartners**. Gezien de ontwikkeldynamiek in technische zin binnen de nieuwe taakvelden en de herschikking van meer verantwoordelijkheden naar de marktpartijen wordt in toenemende mate doelregelgeving, met hierin open normen, opgesteld. Voor ons toezicht betekent dit dat het gesprek over normen en kwetsbaarheden ten aanzien van systemen of menselijk gedrag, plaatsvindt in een vroeg stadium. Dit draagt bij aan een intrinsiek motief om aan de gestelde kwaliteitseisen vanuit de regelgeving en maatschappelijke verwachtingen te voldoen. Daarmee komen we aan de voorkant van de problematiek en dragen we bij aan het vroegtijdig voorkomen of oplossen van systeemfalen.

Autoriteit en toezichthouder

We leven in een gigabitsamenleving. Om te kunnen beantwoorden aan maatschappelijke en technologische uitdagingen, is samenwerking met andere toezichthouders en onafhankelijke onderzoeksinstituten essentieel. Samen vervullen we de rol van **bewaker van het stelsel**. Dit geldt ook voor de internationale samenwerking. Namens Nederland opereren we op een aantal sleutelposities als leider en gids ten aanzien van continuïteit en veiligheid van netwerken en diensten.

Als toezichthouder in het digitaal domein zijn we onafhankelijk in de keuze van de invalshoek en uitvoering van onze programmalijnen en onderzoeken. In aanvulling op onze vertrouwde en traditionele taken, die vooral liggen op het gebied van het gebruik van radiofrequenties voor allerlei toepassingen, richten we ons inmiddels op de beschikbaarheid, bereikbaarheid, veiligheid en betrouwbaarheid van de (digitale) infrastructuur. Hierdoor overzien wij integraal het systeem en speelveld van de techniek in het digitaal domein: de generieke digitale infrastructuur.

Vanuit deze gezaghebbende positie nemen we hierin nu en in de toekomst onze verantwoordelijkheid. Het werk dat Agentschap Telecom verricht, raakt hiermee de hele samenleving.

Deze brochure is een uitgave van:

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen

T +31 (0)50 587 74 44 (ma t/m vrij 8.30 - 17.00)

December 2020 | Publicatie-nr. 20406688