Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Verder bouwen aan een veilige en weerbare digitale infrastructuur

Jaarplan Toezicht 2022
Agentschap Telecom

Voorwoord – Investeren en intensiveren

De Nederlandse digitale infrastructuur wordt bedreigd. Maatschappij en publieke belangen staan onder druk. Dat blijkt onder meer uit het *Cybersecuritybeeld Nederland 2021* en het *Dreigingsbeeld Statelijke Actoren* van de AIVD, MIVD en de NCTV. De dreiging blijft toenemen en de beveiliging weet geen gelijke tred te houden. En dat is uiterst zorgelijk. Want onze samenleving is in hoge mate afhankelijk van de digitale infrastructuur. Daardoor kunnen cyberaanvallen leiden tot zeer ernstige crises.

Digitale technologie stelt Nederland in staat de stap naar de toekomst te maken en maatschappelijke en economische kansen te verzilveren. Helaas gaat dat perspectief gepaard met een toename van de cyberdreiging. Ransomware, Ddos-aanvallen, cyberspionage en alledaagse menselijke fouten kunnen leiden tot verstoringen of uitval van diensten en toepassingen. Dat maakt onze samenleving kwetsbaar. Zeker in de wetenschap dat ook vitale processen ten prooi kunnen vallen aan cybercriminaliteit. Uitval van onze energievoorziening bijvoorbeeld, kan leiden tot een ernstige maatschappelijke crisis. En dat is ook het geval als het bijvoorbeeld telecommunicatie betreft, of toegang tot internet.

De nationale veiligheid vergt additionele inzet en investeringen in cyberweerbaarheid, zo stelt de CSR in het adviesrapport *Integrale aanpak cyberweerbaarheid*. Agentschap Telecom onderschrijft die noodzaak ten zeerste. Het hecht er aan daar aan bij te dragen en intensiveert daarom het toezicht op meerdere fronten.

Dat geldt bijvoorbeeld voor het toezicht op de cyberveiligheid van apparatuur. Inmiddels zijn er naar schatting al zo'n 30 miljard apparaten met het internet verbonden. En dat aantal groeit nog elke dag. Als al die apparaten niet aan de eisen voor cybersecurity voldoen vormen ze in de gezamenlijkheid een gigantisch en gevaarlijk aanvalsoppervlakte voor criminelen. Gelukkig biedt de CE-markering sinds vorig jaar waarborgen op gebied van cyberveiligheid. Dat geeft Agentschap Telecom meer handvatten om onveilige apparatuur uit de handel te houden en van de markt te weren. Aanvullend daarop zal Agentschap Telecom ook zelf – vanuit het eigen IoT-lab – onderzoek doen naar de veiligheid van apparaten. Vooral apparatuur die voorwaardelijk is voor het realiseren van de energietransitie – zoals laadpalen, warmtepompen, zonne-energiesystemen of thuis-accu's – staat daarbij nadrukkelijk in de belangstelling.

Ook vanuit de Europese Cybersecurity Act werken wij aan cyberveiligheid. Als Nationaal Cybersecurity Certificeringsautoriteit (NCCA) kunnen we vanaf 2022 toetsen of processen en producten voldoen aan certificeringsschema's en standaarden voor cyberveiligheid. Nu gebeurt dat nog op vrijwillige basis, mogelijk krijgt het in de toekomst een verplicht karakter.

Het afgelopen jaar heeft Agentschap Telecom meegewerkt aan de totstandkoming van aanvullende wet- en regelgeving om telecommunicatie veilig te houden. Eerdere incidentonderzoeken krijgen in 2022 een vervolg en uitbreiding. Met name de aangescherpte zorgplicht voor telecomsecurity krijgt daarbij nadrukkelijk aandacht.

Maar alle vormen van toezicht ten spijt, voorzorg alleen volstaat niet. Preventieve ingrepen kunnen correctieve maatregelen nooit overbodig maken. Kwetsbaarheid is een gegeven, een zekere mate van risico-acceptatie blijft aan de orde.
Als toezichthouder wil ik daarom investeren in het herstelvermogen van onze digitale infrastructuur. Effectieve rijksbrede samenwerking is daarbij van het grootste belang. Een *digitale grondplaat*, met een helder overzicht van verantwoordelijkheden en competenties, kan daarbij behulpzaam zijn.

Daarnaast zie ik een belangrijke rol weggelegd voor adequaat *business continuity management*. Dat is dan ook een belangrijk onderdeel in ons toezicht op digitale weerbaarheid. Een onderdeel dat we in 2022 als speerpunt onder de Wbni verder uitbouwen. Samen met de sector willen we het collectieve herstelvermogen versterken.

We leven niet in een nul-risico samenleving. Het is zaak goed voorbereid te zijn op incidenten. Weet hoe om te gaan met dreiging, weet hoe te reageren op gevaren, en weet hoe te handelen ten tijde van een crisis. En oefen, oefen en oefen! Dan is herstel niet slechts een reparatie achteraf, maar tegelijkertijd een krachtige voorzorgmaatregel!

Angeline van Dijk
Directeur-hoofdinspecteur Agentschap Telecom

Inhoudsopgave

1

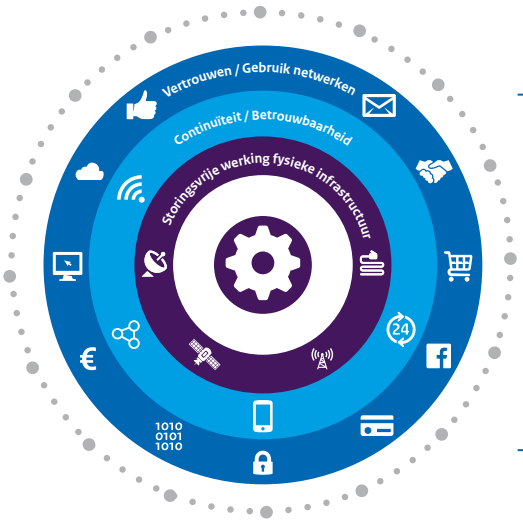
Trends en ontwikkelingen in het digitaal domein

Met de trends en ontwikkelingen die we in dit hoofdstuk beschrijven, geven we een expliciete invulling aan onze signalerings- en agenderingsfunctie.

1.1 Digitalisering; een breed maatschappelijk belang

De Nederlandse samenleving zit in een transitie waarbij digitalisering steeds verder en sterker verweven raakt met bijna alle aspecten van ons dagelijks leven. Het biedt grote kansen voor de maatschappij en economie. De digitale transitie is ook zeker nog niet klaar. We zien meerjarige ontwikkelingen en nieuwe vraagstukken ontstaan. Daarbij speelt een toenemende en diepgaande maatschappelijke afhankelijkheid van digitalisering en tegelijkertijd een toename van dreigingen en (potentiële) verstoringen. Het is dan ook niet voor niets dat de samenleving moet kunnen vertrouwen op een onafhankelijke toezichthouder die maatschappelijke vraagstukken rond de digitale infrastructuur detecteert, kwetsbare belangen beschermt en vroegtijdig risico's onderkent.

Agentschap Telecom is die toezichthouder. Wij staan middenin de samenleving en ontwikkelen ons tot *autoriteit voor de digitale infrastructuur*. Ons toezicht is erop gericht dat Nederland kan vertrouwen op de beschikbaarheid van de digitale infrastructuur, die continu en veilig te gebruiken is. Daarbij richten we ons op de volgende vraagstukken:



Is de infrastructuur aangelegd, verbonden en weerbaar?

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

Werken de apparaten en instrumenten goed en veilig?

De traditionele onderwerpen van ons toezicht zoals telecom, radiofrequenties, veilig graven en meetsystemen zijn geïntegreerd in ons toezicht op de beschikbaarheid, bereikbaarheid, veiligheid en betrouwbaarheid van de (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' borgt de integriteit van de digitale infrastructuur en omvat tevens de deels analoge onderliggende infrastructuur.

1.2 Digitale infrastructuur; complex en dynamisch

De complexiteit en dynamiek van het digitaal domein nemen verder toe. Nieuwe digitale toepassingen en verbindingen tussen ketens en ecosystemen worden tot stand gebracht. De verschillende ketens gaan elkaar overlappen. En hoewel er steeds meer mogelijk is, blijkt ook dat niet àlles kan. Nieuwe ontwikkelingen, diensten en producten kunnen qua aard en omvang de beschikbare infrastructuur overvragen; dat vraagt om een nieuwe balans, maar ook om een andere rol van ons als toezichthouder. Stakeholders uit diverse sectoren hebben een toenemende behoefte om ons naast de (technische) inhoud te bevragen op regie en coördinatie in complexe en dynamische vraagstukken.

In deze ontwikkeling zien wij dan ook een veranderende maatschappelijke opgave. Wij kunnen daarin een (regie)rol pakken en beïnvloeden door complexiteit in (en tussen) ketens te ontrafelen, 'onder de motorkap te kijken' om een technisch expertoordeel te geven en door stakeholders te activeren. Die rol zien we bijvoorbeeld bij het vraagstuk rond de energietransitie in samenhang met de digitale transitie, waarbij de toenemende cyberdreiging ook een rol speelt.

Digitalisering & Energietransitie

Als Nederland de klimaatdoelen wil halen, dan moet er op korte termijn geïnvesteerd worden in (de veiligheid van) de bijbehorende digitale infrastructuur en apparatuur. Denk bijvoorbeeld aan warmte-, waterstof- en elektriciteitsnetten, elektrische auto's, laadpalen, energiemeters en zonnepanelen. De energieambities leunen daar immers sterk op. De beschikbaarheid, weerbaarheid, continuïteit/integriteit en veiligheid van de infrastructuur en apparatuur in het energiedomein zijn dan ook van vitaal belang voor de samenleving. De samenloop van de energie- en digitale transitie brengt diverse (nieuwe) risico's aan het licht die meerdere onderwerpen van ons toezicht raken.

Cyberrisico's

Door de toenemende digitalisering in de energiesector nemen de cyberrisico's toe. Door gehackte apparatuur massaal en gelijktijdig in- of uit te schakelen kan overbelasting op het energienet gecreëerd worden. Dat kan uiteindelijk leiden tot uitval. Ook het gebruik van kunstmatige intelligentie (AI), bijvoorbeeld voor het aansturen en bewaken van de energiebalans op het net geeft kansen, maar kent ook risico's.

Risico's stoorsignalen

Zonnepaneelinstallaties zijn cruciaal voor de energietransitie. In het jaarbericht 2020 meldden we al dat ze storing kunnen veroorzaken op andere apparatuur. Als de ondersteunende regelende componenten ondeugdelijk zijn gefabriceerd, onjuist gebruikt worden of foutief zijn geïnstalleerd, kunnen ze stoorsignalen uitzenden die er toe kunnen leiden dat andere apparaten en diensten niet meer goed functioneren.

Risico's voor het meten en afrekenen van energieverbruik

Door de energie- en digitale transitie gaan consumenten en bedrijven op een andere wijze energie afnemen en afrekenen. Denk aan slimme meters, het opladen van een elektrische auto aan een laadpaal of het meten van het gebruik van waterstof. Het meten en registreren van dat energieverbruik moet net zo veilig en betrouwbaar zijn als bij het traditionele 'tanken aan de pomp'.

Verhoogd risico op graafschade

In verband met de energietransitie moeten er nieuwe kabels en leidingen onder de grond gelegd worden. Dat is nodig om elektriciteitsnetten uit te breiden of te verzwaren, of voor de aanleg van warmte- of waterstofnetten. Maar graven is niet zonder risico. Onzorgvuldig graven kan leiden tot schade aan kabels en leidingen die al in de grond liggen. De graafsector is er de afgelopen jaren nog niet in geslaagd de graafschades te verminderen. Dat is zorgelijk, omdat de energietransitie zal leiden tot nog meer graafwerkzaamheden.

Inzicht en onderzoek

We willen meer en beter inzicht krijgen in de mogelijke (maatschappelijke) risico's van de energietransitie, zodat deze vroegtijdig aangepakt kunnen worden en niet tot onnodige problemen of vertraging in de transitie zullen zorgen. Daarom doen we onder andere onderzoek naar de toepassing en impact op de elektriciteitsketen en de risico's van elektrische apparatuur die zowel aan het elektriciteitsnet als het internet gekoppeld is (zoals laadpalen, warmtepompen, zonne-energiesystemen of thuis-accu's). Vanuit nationale en internationale gremia werken we aan de standaardisatie van cyberveilige apparatuur en diensten. Bovendien intensiveren we ons onderzoek naar mogelijk verstorende apparatuur. Indien nodig halen we verstorende apparatuur van de markt. Zo pakken we als toezichthouder onze eigen verantwoordelijkheid in de energietransitie.

Om de energietransitie onder invloed van digitalisering succesvol te laten zijn, is er meer nodig. Dat vraagt om een integrale benadering van geïdentificeerde risico's, vanuit alle drie de ringen van de digitale infrastructuur. Nieuwe en bestaande vraagstukken vragen ook om integrale afstemming en samenwerking met partijen binnen de overheid en het bedrijfsleven, zowel nationaal als internationaal. Daarvoor is het opstellen van een *digitale grondplaat*, waarmee de totale governance van het digitale stelsel van beleid, uitvoering en toezicht in kaart wordt gebracht, behulpzaam. Daarmee worden verantwoordelijkheden, afhankelijkheden en eventuele hiaten zichtbaar. Er is een gezamenlijke verantwoordelijkheid om ervoor te zorgen dat het systeem werkbaar is en er effectief wordt samengewerkt.

Beschikbaarheid en zorg infrastructuur voor 5G

Een andere belangrijke ontwikkeling voor de digitale infrastructuur is 5G, de opvolger van 4G. Ten opzichte van 4G brengt 5G extra mogelijkheden voor onze mobiele communicatie. Mobiele communicatie in het algemeen – en 5G in het bijzonder – maakt talloze innovaties in de industrie, zorg en landbouw mogelijk. Agentschap Telecom zet zich op verschillende fronten in voor beschikbare, betrouwbare en veilige connectiviteit in Nederland.

In 2020 zijn vergunningen geveild die mobiele communicatie via 5G mogelijk maken. In de vergunningen zijn dekking- en snelheidsverplichtingen (DSV) opgenomen om de beschikbaarheid van de benodigde infrastructuur te borgen en consumenten en bedrijven toegang te bieden tot een vastgesteld minimaal serviceniveau. De eisen zien op het stapsgewijs bereiken van 98% dekking en een snelheid van 8 Mbit/sec. De vergunninghouders dienen per 1 juli 2022 de eerste verplichting na te komen. Wij gaan gericht toezicht houden op de naleving van de DSV om de beschikbaarheid van infrastructuur voor 5G te bevorderen.

Door de extra vraag naar mobiele communicatie zal het aantal antennes toenemen. Dat leidt bij sommigen tot zorg over blootstelling aan elektromagnetische velden en gezondheid. Een zorg die Agentschap Telecom serieus neemt. Daarom houden we de vinger aan de pols. Zo gaan we in 2022 het aantal veldsterktemetingen bij antennes intensiveren en richten op specifieke locaties in de nabijheid van bijvoorbeeld scholen, winkelcentra en ziekenhuizen.

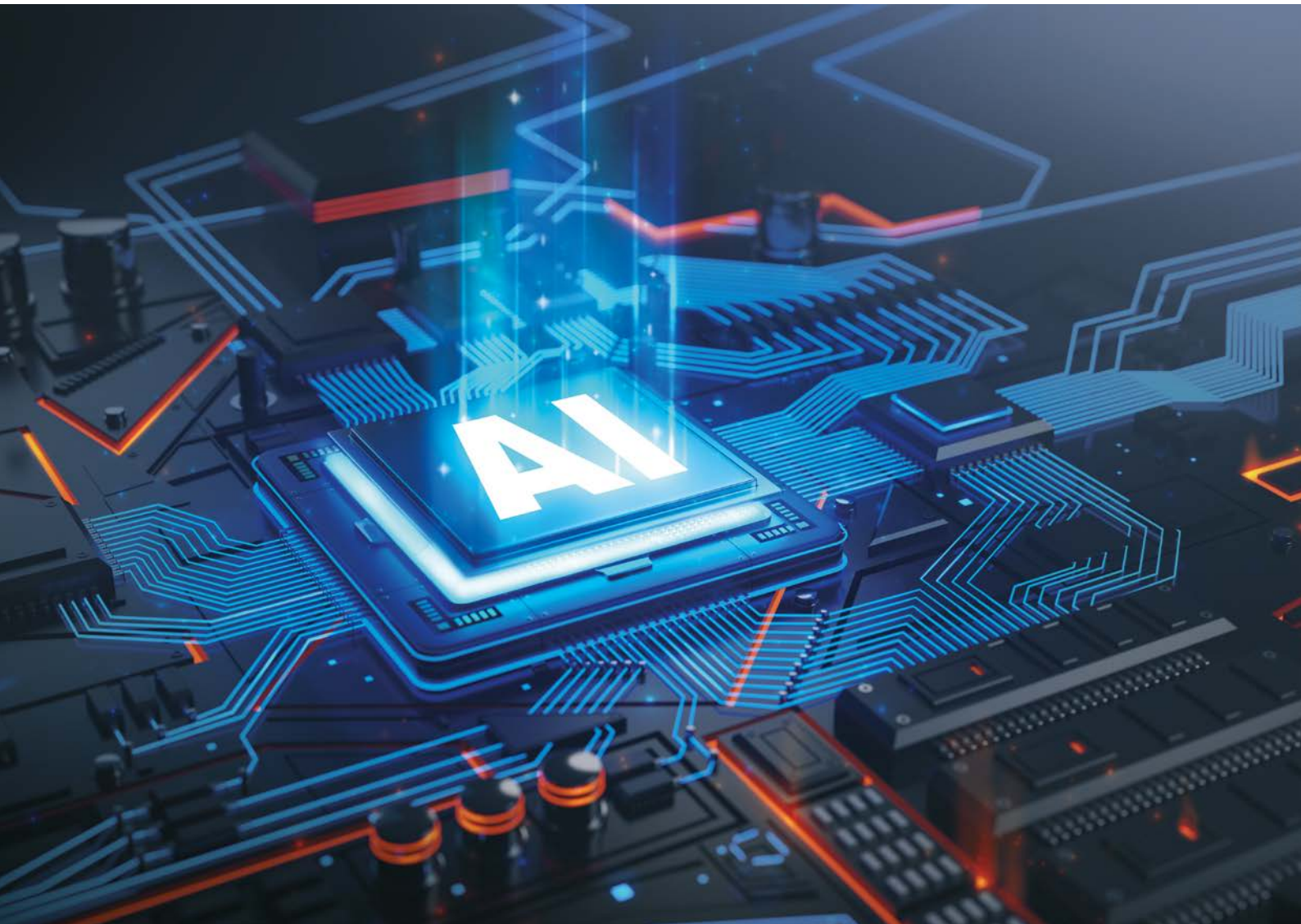
Artificiële Intelligentie (AI)

De grote maatschappelijke en economische belangen die spelen bij de kansen en risico's van AI zijn door het kabinet onderstreept in haar voortgangsbrief aan de Tweede Kamer van 10 juni 2021. Het kabinet wil risico's voor publieke waarden en fundamentele rechten beperken door (onder meer) versterking van het toezicht, de samenwerking tussen toezichthouders en de samenhang in toetsingskaders voor AI. De Wetenschappelijke Raad voor Regeringsbeleid (WRR) heeft daarnaast op 11 november 2021 een belangrijk advies uitgebracht aan de regering. De WRR concludeert dat de overheid zich actiever moet voorbereiden op een samenleving waarin AI een grote rol speelt. Alleen wanneer de overheid haar opgaven structureel ter hand neemt, kan zij de publieke waarden die gemoeid zijn met de inzet van AI ook in de toekomst beschermen en garanderen.

De koers die we vanaf 2019 hebben ingezet op AI, sluit naadloos aan op de kabinetskoers en het WRR-advies.
Op ons initiatief en voorzitterschap is – ondersteund door Bureau Inspectieraad – de samenwerking met andere toezichthouders verstevigd door de vorming van een interdepartementale werkgroep Toezicht op AI/algoritmen. De werkgroep heeft als doel om kennis uit te wisselen, van elkaar te leren en de aanpak te harmoniseren. Dat is essentieel om Nederland het vertrouwen te blijven geven in het veilig gebruik van kunstmatige intelligentie.

We zijn ook internationaal actief voor de veiligheid van op AI-gebaseerde systemen en oplossingen. Zo zijn we lid van de AI-werkgroep van ETSI dat met het rapport *AI Problem Statement* een belangrijke eerste stap heeft gezet naar een wereldwijde standaardisatie voor het veilig toepassen van artificiële intelligentie. Ook zijn we actief richting de Europese Commissie. We waren we in 2020 betrokken bij een whitepaper waarin de Europese Commissie haar visie geeft op de ontwikkeling van beleid en regelgeving op het gebied van AI. Daarnaast hebben we het initiatief genomen om de Europese toezichthouders op het thema AI bij elkaar te brengen met als doel kennisuitwisseling en delen van best practices.

Naast een (inter)nationale voortrekkers- en regierol houden we op dit moment al toezicht op AI toepassingen in de verschillende toezichtsdomeinen.



1.3 Digitale infrastructuur; weerbaarheid en veiligheid vragen constante inzet en alertheid

Er zijn in de afgelopen periode op een aantal terreinen de nodige stappen gezet voor een veilige en weerbare digitale infrastructuur, diensten en processen. Er is in de breedte nog veel werk aan de winkel en dat werk is nooit af. Er is voortdurende alertheid, adequaat handelen en scherpte nodig omdat de aard van dreigingen en digitale risico's toeneemt. Het *Cyber Security Beeld Nederland 2021* laat zien dat vrijwel alle vitale processen en diensten volledig afhankelijk zijn van digitale infrastructuur.

De grootste actieve dreiging komt vanuit *statelijke actoren* die door spionage, sabotage en verstoring langdurig impact kunnen hebben op digitale systemen en processen van de (vitale) digitale infrastructuur. Ze kunnen bijvoorbeeld via een achterdeur toegang krijgen tot een netwerk en daar ongezien verblijven. Daarbij verkennen ze de systemen en creëren ze nieuwe toegangen.

Cybersecurity-experts signaleren grote verschillen in weerbaarheid in Nederland. Kleine bedrijven, bijvoorbeeld in het MKB, beschikken regelmatig niet over de expertise en de middelen om de weerbaarheid naar een hoger plan te tillen. Zij kunnen doelwit zijn, bijvoorbeeld als ze deel uitmaken van de leveranciersketens van andere (ook vitale) processen. Naast voornoemde actieve dreiging, is onbedoelde uitval van systemen als gevolg van technische mankementen of menselijk handelen nog steeds de meest voorkomende oorzaak van uitval van netwerken en systemen. Weerbaarheid is dus noodzakelijk op alle niveaus in een organisatie.

Weerbaarheid en herstelvermogen

Bij de door de overheid aangewezen vitale organisaties, zoals telecomoperators en energieproducenten, zien we dat er voldoende bewustzijn aanwezig is van het belang van digitale weerbaarheid en cybersecurity. Dat is geenszins een reden om achterover te leunen. In het licht van toenemende dreigingen en digitale afhankelijkheden in toeleverantie en ketens is adequaat Business Continuity Management (BCM) van groot belang om te voorzien in continuïteit en robuustheid van netwerk- en informatiesystemen. In 2022 hebben we in ons toezicht op weerbaarheid en cybersecurity bijzondere aandacht voor BCM en zullen daarbij tevens een focus hebben op Supply Chain Management (SCM).

Want om weerbaar te zijn, is het belangrijk om niet alleen na te denken over preventieve beveiligingsmaatregelen in de vorm van Information Security Management (ISM), maar ook over (aanvullende) maatregelen voor het herstelvermogen en incidentafhandeling van een organisatie: BCM dat ziet op veerkracht, responscapaciteit en herstelvermogen. Het is niet de vraag óf je kwetsbaar bent, maar wannéér je geraakt wordt door bedoelde of onbedoelde uitval. Dit kwam bijvoorbeeld ook naar voren in een onderzoek dat TNO in opdracht van het Nationaal Cyber Security Centrum heeft gedaan naar het herstelvermogen binnen IT- infrastructuren.

Door toenemende digitale afhankelijkheden in toeleverantie en ketens zien wij een belangrijke rol voor adequaat Business Continuity Management.
Dit heeft dan ook een belangrijke plaats in ons toezicht op digitale weerbaarheid. Ook is collectief herstelvermogen, het samenwerken op het gebied van herstelvermogen bij supply-chains of sectorbreed in de ketens van belang.

Het belang van verdere verbetering van de veerkracht en responscapaciteit van (vitale) digitale infrastructuren is ook ingezien door de Europese Commissie. Zij heeft een voorstel gedaan voor een nieuwe richtlijn, *de NIS2 richtlijn*, ter vervanging van de oorspronkelijke NIS-richtlijn. Daarmee wil zij onder meer de cyberveerkracht van bedrijven in alle relevante sectoren vergroten, verschillen in de veerkracht beperken en de gemeenschappelijke kennis en collectieve paraatheid en responscapaciteit vergroten. Op basis van de concepten van de NIS2-Richtlijn uit 2021, is de verwachting dat er meer aanbieders van essentiële diensten worden aangewezen in ons toezichtsdomein. Ook de aankomende *EU Netwerkcode cybersecurity elektriciteitssector* lijkt gevolgen te kunnen hebben voor de aard en omvang van ons toezicht op cybersecurity in de elektriciteitssector. Daarbij zien we een samenhang met de NIS2-richtlijn.

Digitaal veilige apparatuur

Het aantal apparaten dat met internet verbonden is, is de laatste jaren snel gegroeid. Voorbeelden daarvan zijn thermostaten, horloges, babyfoons en speelgoed. Of robots en slimme sensoren in de industrie. Naar schatting zijn er wereldwijd inmiddels al zo'n 35 miljard apparaten met internet verbonden. Het Internet of Things (IoT) is inmiddels een realiteit en er zullen naar verwachting in 2030 zelfs al 125 miljard apparaten 'online' zijn.

Dat brengt veel extra mogelijkheden, functionaliteit en gebruiksgemak. Maar als de digitale veiligheid van apparatuur niet op orde is, brengt het ook risico's met zich mee. Het 'aanvalsoppervlak' voor hackers neemt met het toenemend aantal IoT-apparaten namelijk snel toe. Dat kan niet alleen gevolgen hebben voor het veilig en betrouwbaar functioneren van het apparaat, maar ook een bredere negatieve uitwerking hebben naar de digitale infrastructuur. Denk daarbij bijvoorbeeld aan het misbruiken van onveilige IoT-apparaten voor massale DDOS-aanvallen.

De Europese Commissie heeft daarom besloten dat er verplichte veiligheidseisen komen voor slimme apparaten. Daarmee moet (beter) worden voorkomen dat slimme apparaten kunnen worden gemanipuleerd, privacy gevoelige data kunnen prijsgeven of besmet kunnen raken met malware. De nieuwe eisen zijn onderdeel van de *Radio Equipment Directive*. Deze Europese richtlijn bestond al – en stelde al eisen aan andere aspecten van apparaten – bijvoorbeeld op gebied van gezondheid, elektrische veiligheid en storingsgevoeligheid. Apparaten die aan alle eisen voldoen, mogen de bekende CE-markering dragen. Vanaf medio 2024 geldt de CE-markering dus ook voor de digitale veiligheidseisen. Apparaten die er niet aan voldoen, krijgen geen toegang tot de Europese markt en moeten worden geweerd. Wij gaan ook op de naleving van de digitale veiligheidseisen toezien, bij overtredingen sanctioneren en digitaal onveilige apparaten uit de handel halen. Wij gaan daarom al starten met de voorbereiding van het toezicht op de nieuwe veiligheidseisen voor slimme apparaten.

De afgelopen periode hebben we hard gewerkt aan het ontwerp en de inrichting van ons IoT-testlab. Nu dat operationeel is, vormt het een waardevolle tool voor ons toezicht op de cyberveiligheid van IoT-apparatuur.

Veiligheid en integriteit telecommunicatie

Ten aanzien van de weerbaarheid van de digitale infrastructuur speelt ook de politieke en maatschappelijke aandacht voor de veiligheid en integriteit van telecommunicatie. Om te borgen dat burgers en bedrijven in Nederland altijd en overal kunnen rekenen op betrouwbare en veilige mobiele telecominfrastructuur, zijn recent concrete beveiligingseisen van kracht geworden om bijvoorbeeld spionage en misbruik via kritieke systeemcomponenten te voorkomen. Telecomaanbieders moeten daar voor 1 oktober 2022 aan voldoen. Wij gaan het toezicht op de verplichte eisen met prioriteit verder inrichten en daarna starten met de uitvoering van gerichte inspecties.

Uitbreiding Telecomcode met OTT-diensten

De nieuwe Europese richtlijn voor telecom, de *Telecomcode (EECC)*, is de herziening van Europese regels op telecomgebied. Deze code zal naar verwachting in januari 2022 geïmplementeerd worden in de Telecommunicatiewet. Eén van de gevolgen van implementatie is dat de nummeronafhankelijke interpersoonlijke communicatiediensten (ook wel bekend als Over The Top (OTT)-diensten, zoals Whatsapp en Skype) onder ons toezicht gaan vallen. De zorg- en meldplicht is bovendien uitgebreid: het is verplicht om maatregelen te nemen om de risico's voor de beveiliging van netwerken of diensten te beheersen en significante incidenten te melden. Onder beveiliging valt de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van netwerken en diensten.

Cyber Security Act

De *Cyber Security Act (CSA)* is een Europese verordening die tot doel heeft om het niveau van cyberbeveiliging in de Europese Unie te verhogen en de beveiligingseisen voor IT-producten, -diensten en -processen te harmoniseren. Fabrikanten en dienstverleners dienen adequate maatregelen te nemen om de cyberveiligheid van hun producten, systemen en diensten te borgen. Daartoe definieert de CSA een Europees certificeringstelsel en het toezicht daarop. De lidstaten worden geacht een of meerdere organisaties aan te wijzen die de taak van Nationale Cybersecuritycertificeringsautoriteit (NCCA) uitvoeren.

We bereiden ons – als beoogd toezichthouder – voor op de NCCA-taken en maken deel uit van de Europese adviesgroep. We leveren met inzet van eigen experts een actieve bijdrage aan het tot stand komen van de certificeringsschema's. Naar verwachting zullen deze taken over de tijd in omvang gaan toenemen. Mede door het nog vrijwillige karakter van de certificering is het tempo en de omvang van de groei niet voorspelbaar. In 2022 gaan we het toezicht op cyberveiligheidscertificatieschema's en certificeringsbeoordelingsinstanties inrichten.

2

Programmering Toezicht 2022

In lijn met de trends, ontwikkelingen en onze risicoschatting, zet Agentschap Telecom voor 2022 in op de onderstaande programmering van haar toezicht[1]:

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

Energietransitie en Digitale transitie

Telecomsecurity

Kwaliteit en betrouwbaarheid mobiele netwerken

Meerdere domeinen overstijgend is het thema **energietransitie in combinatie met de digitale transitie** voor ons topprioriteit. Waarbij we oog hebben voor de steeds verdergaande afhankelijkheid tussen energievoorzieningen en de digitale infrastructuur en de bijbehorende cyberweerbaarheid van deze infrastructuren. Energietransitie en digitale transitie versterken elkaar.

Het toezicht op de aangescherpte zorgplicht ten aanzien van de **telecomsecurity** wordt verder vormgegeven. Mede naar aanleiding van een incidentonderzoek in 2021 wordt de telecomsecurity als prioritair thema in ons toezicht gepositioneerd.

Het derde thema betreft de kwaliteit en betrouwbaarheid van mobiele netwerken waarbij de naleving van **de dekkings-en snelheidseisen ten aanzien van 5G** een belangrijk onderwerp is. De nieuwe vergunningen moeten in gebruik genomen worden en voldoen aan de vergunningseisen, zodat zoveel mogelijk mensen en bedrijven kunnen beschikken over veilige en snelle mobiele dataverbindingen.

We blijven ons toezicht intensiveren op apparaten. Dat is elementair voor het vertrouwen in de digitalisering die cruciaal is voor de economische positie van Nederland. **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.

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.

[1] 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.

Publiek Belang **Goede dekking en een optimale capaciteit van mobiele netwerken.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Niet iedereen kan gebruik maken van sneller mobiel internet.	Een optimale dekking en snelheid van mobiele netwerken. Kwaliteit en betrouwbaarheid mobiele netwerken	Inrichting toezicht ten aanzien van de dekking- en snelheidsverplichting (DSV), in de 2e helft van 2022 gevolgd door gerichte inspecties waar risico's ten aanzien van de DSV het grootst zijn.

Publiek Belang **Continuïteit en veiligheid van bedrijfsprocessen bij het gebruik van draadloze communicatie in de industrie en MKB.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Verstoringen communicatie-netwerken in belangrijke sectoren, vanuit economisch en veiligheids-oogpunt bezien.	Ongestoord frequentiegebruik van vergunninghouders in de land-mobiele sector (o.a. BRZO-bedrijven). Kwaliteit en betrouwbaarheid mobiele netwerken	Continueren programmatische aanpak gericht op verbetering van het landmobiele radiolandschap via interventies op systeemniveau met in 2022 de focus op vergunning-houders.

Publiek Belang **Acceptabele kwaliteit van het radiolandschap.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Technische kwaliteit van de omroep-uitzendingen neemt af en/of storingen bij gebruik van vitale radiofrequenties. Niet iedereen kan ongestoord luisteren naar radio-uitzendingen.	Luisteraars moeten DAB+ zenders ook daadwerkelijk kunnen ontvangen. Voorkomen en opheffen van verstoringen bij reguliere vergunninghouders en vitale frequentiegebruikers.	Risico's op verstoring huidige systemen vroegtijdig mitigeren en gelijk speelveld borgen door actieve communicatie, voorlichting en kennismakingsgesprekken bij en met nieuwkomers FM en DAB+. In samenwerking met de ketenpartners monitoren/opsporen illegale zenders in de FM-band met oog op bewaken kwaliteit van het radiolandschap. Uitvoeren ketentoezicht in twee specifieke regio's en dit tevens uitrollen naar andere regio's.

Publiek Belang **Beschikbare netwerken voor vitale overheden.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Verstoring van netwerken als gevolg van toenemend gebruik van radarsystemen.	Volledig inzicht krijgen in de afhankelijkheden en risico's van radarsystemen.	Uitvoeren onderzoek in volle breedte ten aanzien van technische parameters en veiligheid van radarsystemen.

Publiek Belang **Leveringszekerheid van vitale diensten zoals energie, gas, water en telecom/ internet.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
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. Energietransitie en Digitale transitie	Agentschap Telecom start een project met het KLO om te komen tot één generieke werkinstructie waarin de minimale vereisten voor het graafteam zijn opgenomen, op basis van het maatregelenplan van de opdrachtgever. Minimaal 10 ketenonderzoeken naar aanleiding van graafschade aan een gasleiding, waarbij de rol en gedragingen van grondroerder en opdrachtgever in het specifieke geval worden onderzocht.

2.3 Toezicht op security en weerbaarheid van netwerken en diensten

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

Naast beschikbaarheid van technische infrastructuren, wordt op basis van de aangescherpte zorgplicht het toezicht op de continuïteit en integriteit van telecomnetwerken en diensten geïntensiveerd. Zowel vanuit het aspect van telecomsecurity als cyberweerbaarheid. Netwerken dienen zo adequaat mogelijk beschermd te zijn tegen uitval en manipulatie veroorzaakt door externe factoren. Het kan daarbij bijvoorbeeld gaan om het noodnummer 112 en de telecommunicatiesector, maar ook om de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. Nu de regelgeving zowel Europees als nationaal scherper is geformuleerd zal Agentschap Telecom haar toezicht daarmee intensiveren. Agentschap Telecom ziet toe op de borging van de cyberweerbaarheid van vitale infrastructuur door 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	*Toezichtdoel 2022*	*Speerpunten 2022*
De burger kan 112 niet bereiken of wordt niet bereikt door NL-alert berichtgeving op drukbezochte locaties.	Continuïteit van dienstverlening NL-alert en 112, ook bij grote evenementen. Kwaliteit en betrouwbaarheid mobiele netwerken Telecomsecurity	Monitoring en onderzoek beschikbaarheid en bereikbaarheid van 112 bij grote evenementen (zoals Vuelta en Formule 1) om bewustwording en gezamenlijke verantwoordelijkheid te stimuleren.

Publiek Belang **Burgers en bedrijven kunnen ongestoord gebruik maken van telecomdiensten.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
De integriteit en veiligheid van netwerken wordt bedreigd door het gebruik van ongewenste systeemcomponenten.	Aanbieders treffen adequate maatregelen om de integriteit en veiligheid van hun netwerken en diensten te borgen. Telecomsecurity	Inspecties bij de mobiele netwerkoperators op het gebied van telecomsecurity (veiligheid en integriteit) van kritieke onderdelen van telecommunicatienetwerken. Daarbij richten we ons specifiek op: • naleving van de eisen aan de ministeriële Regeling veiligheid en integriteit telecommunicatie; • monitoring van de programma's om tijdig te voldoen aan de besluiten onder de AMvB veiligheid en integriteit telecommunicatie.

Publiek Belang **Beschermen van de continuïteit van diensten die van cruciaal belang zijn voor consumenten en bedrijven ter voorkoming van digitale ontwrichting.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Onvoldoende cyberweerbaarheid in de keten van vitale infrastructuren.	Aanbieders (van essentiële diensten en digitale dienstverleners) treffen adequate maatregelen op het terrein van Supply-Chain Management (SCM) en Business Continuity Management (BCM), met als doel de cyberweerbaarheid van vitale infrastructuren te borgen. Energietransitie en Digitale transitie	Risicogerichte thema-inspecties op het onderwerp BCM ten aanzien van de netwerk- en informatiesystemen van vitale aanbieders (AED) in de sectoren energie en digitale infrastructuur. Algemene aandacht en verdieping op het thema SCM in de sectoren energie en digitale infrastructuur.
	Aanbieders van digitale diensten (DSP's) hebben een adequaat niveau van security-bewustzijn. Energietransitie en Digitale transitie	Stimuleren van DSP's om een door Agentschap Telecom ontwikkeld online self-assessment uit te voeren ten aanzien van hun digitale weerbaarheid.
	Volgen en duiden van complexiteit en dynamiek ten aanzien van security en weerbaarheid. Kwaliteit en betrouwbaarheid mobiele netwerken Energietransitie en Digitale transitie	Versterken van de samenwerking en kennisdeling met collega toezicht-houders over de betekenis van Artificial Intelligence (AI) in termen van security en weerbaarheid.

Publiek Belang **Beschermen van de continuïteit van diensten die van cruciaal belang zijn voor consumenten en bedrijven ter voorkoming van digitale ontwrichting.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
De kwaliteit van het certificerings-proces is onvoldoende om de cyberveiligheid te kunnen borgen.	Fabrikanten en dienstverleners treffen adequate maatregelen om de cyberveiligheid van hun producten, systemen en diensten te borgen. Energietransitie en Digitale transitie Kwaliteit en betrouwbaarheid mobiele netwerken	Inrichting van het toezicht op cyberveiligheidscertificerings-schema's en -regelingen en conformiteit-beoordelingsinstanties op basis van de Cyber Security Act.

Publiek Belang **Beschermen van de continuïteit en integriteit van IT-diensten op Europees niveau.**		
Risico	*Toezichtdoel 2022*	*Speerpunten 2022*
Door incongruentie in de diverse nieuwe Europese richtlijnen zijn er onvoldoende waarborgen ten aanzien van continuïteit en integriteit van netwerken en diensten.	Hoog niveau van continuïteit en veiligheid van netwerken en diensten door een gecoördineerde inbreng vanuit de gezamenlijke Europese toezichthouders. Kwaliteit en betrouwbaarheid mobiele netwerken Telecomsecurity Energietransitie en Digitale transitie	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. In samenwerking met andere lidstaten de grote toename aan Europese regelgeving op het gebied van continuïteit, integriteit van IT-diensten stroomlijnen.

2.4 Toezicht op veilige apparaten

Werken de apparaten en instrumenten goed en veilig?

In toenemende mate vervagen de klassieke grenzen tussen soorten apparatuur. Veel apparatuur is inmiddels draadloos verbonden met het internet, wat cyberrisico's met zich meebrengt. De energietransitie stimuleert energiezuinige apparatuur maar deze veroorzaken vaker storingen in de ether. Sinds het voorjaar van 2020 is de productverkoop via e-commerce onder invloed van de coronapandemie enorm gestegen. Dit vraagt om een andere vorm van toezicht waarbij samenwerking met collega-toezichthouders en de marktdeelnemers een belangrijke rol krijgt. Bij het toezicht op het gebruik en veiligheid van apparaten gaat het met name om eerlijke handel en het bevorderen van vertrouwen in het veilig gebruik van apparatuur die goed werkt. Dat gaat niet alleen maar om de apparaateigenschappen (werking, storingsgevoeligheid, elektromagnetische straling), de veilige werking en robuustheid tegen digitale bedreigingen maar ook om betrouwbare hoeveelheidsinformatie van bijvoorbeeld weegschalen, kilowattuurmeters en benzinepompen.

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	*Toezichtdoel 2022*	*Speerpunten 2022*
Storingen en (cyber)onveilige situaties kunnen ontstaan door ondeugdelijke apparatuur of software.	Fabrikanten, importeurs en distributeurs brengen apparatuur op de markt die aan de wettelijke eisen voldoet. Gebruikers beschikken daarmee over veilige en betrouwbare apparaten en meetinstrumenten. Kwaliteit en betrouwbaarheid mobiele netwerken Energietransitie en Digitale transitie	Onderzoek naar productgroepen met grootste risico's op het gebied van verstoringen, storingsgevoeligheid, elektrische- en cyberveiligheid. Intensivering onderzoek (onder meer met inzet van ons IoT-testlab) naar, en brancheoverleg over cyberveiligheid IoT-producten. Het bieden van handelingsperspectieven aan gebruikers van vergunningvrije toepassingen voor de meest voorkomende storingsproblemen. Starten van systeemtoezicht bij fabrikanten en importeurs met een uitgebreid assortiment. Verdere intensivering EMV-metingen bij de verdere bouw van 5G-infrastructuur, met bijzondere aandacht voor specifieke locaties.
Meetinstrumenten die worden gebruikt bij handelstransacties meten niet goed.	De metrologische aspecten van de energietransitie worden geborgd. Energietransitie en Digitale transitie	Inrichten basistoezicht op gebruikers van laadpalen (charge point operators). Informeren van gebruikers van waterstofdispensers over de metrologische eisen aan nieuw geplaatste dispensers en het inrichten & uitvoeren van het toezicht daarop. Inrichten van toezicht op gebruikers van warmtemeters.

3

Ons toezicht

We houden toezicht met als doel om publieke belangen te borgen en maatschappelijke risico's te mitigeren.
Dat doen we 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.

Een integrale aanpak

Agentschap Telecom ontwikkelt zich tot **autoriteit voor de digitale infrastructuur**. Ons toezicht is erop gericht dat Nederland kan vertrouwen op de beschikbaarheid van deze digitale infrastructuur, die continu en veilig te gebruiken is. Ons werkveld kenmerkt zich door een beleidsdomeinen-overstijgend karakter. Een voorbeeld hiervan is het energietransitie-vraagstuk in samenhang met de digitale transitie, maar ook de toenemende cyberdreiging.

De gehele samenleving digitaliseert. Hierdoor ontstaan nieuwe, generieke vraagstukken, breder dan bijvoorbeeld privacy alleen. We zien een toenemende en diepgaande maatschappelijke afhankelijkheid en verknoping van verschillende vormen van digitalisering en tegelijkertijd een toename van dreigingen en (potentiële) verstoringen.

De nieuwe en bestaande vraagstukken vragen om uitgebreide afstemming en samenwerking, in het beleid, in de uitvoering, en in het toezicht. We werken daarom samen met partijen binnen de overheid en het bedrijfsleven, zowel nationaal als internationaal. Een integrale aanpak is noodzakelijk, waarbij wordt gewerkt vanuit de maatschappelijke opgave en de te beschermen publieke belangen in plaats van vanuit een wettelijke of formeel organisatorische begrenzing.

Dit vraagt om een *transitie in het denken en handelen van alle betrokken partijen*. Silo-denken moet plaatsmaken voor de netwerkgedachte, waarbij de opgave centraal staat en niet de taak. Een zekere flexibiliteit is nodig, waarbij naar gelang de opgave vanuit wisselende coalities binnen het digitale ecosysteem wordt samengewerkt. Dit geldt voor de bestaande instituten, maar ook voor potentiële nieuwe partners.

Autoriteit en toezichthouder

Door een integrale aanpak vervullen verschillende beleidsdomeinen, toezichthouders, kennisinstituten samen de rol van **bewaker van het stelsel**. Een systematische blik, waarbij elke betrokken organisatie vanuit haar kennis en expertise een bijdrage levert. Namens Nederland opereren we op een aantal sleutelposities als leider en gids ten aanzien van continuïteit en veiligheid van netwerken en diensten. Het voorrecht van Agentschap Telecom hierin is dat we in staat zijn ook de diepgaande onderliggende techniek te doorgronden en te beoordelen op eventuele risico's ten aanzien van de continuïteit en (cyber) veiligheid. Deze autoriteitspositie stimuleert ons om te blijven investeren in het behouden en halen van goed opgeleid specialistisch personeel.

Bovendien mag de maatschappij van ons als toezichthouder verwachten dat we consistent en consequent optreden als we bij de uitvoering van ons toezicht omissies constateren die publieke belangen schaden of maatschappelijke risico's veroorzaken. *Met kennis van zaken creëren we beweging tot naleving.* Daarvoor hebben we een breed palet aan instrumenten om effectief te kunnen zijn. Maatregelen als informele (gedrags) interventies alsook formele handhaving met boetes en lasten onder dwangsom zullen worden ingezet om het gewenste nalevingseffect te bereiken.

Kernwaarden

Onze kernwaarden geven ons houvast, samenhang en richting voor onze werkprocessen, besluitvorming en maatschappelijke positionering. Daarmee helpen ze ons in de ontwikkeling van een taakgerichte naar een doelgerichte organisatie, die handelt vanuit de maatschappelijke opgave. Wij hanteren de volgende kernwaarden: *maatschappelijke verantwoordelijkheid, gedeelde visie, samenwerking, verantwoordelijkheid nemen en professionaliteit*.

Toezichtvisie

Onze toezichtvisie sluit naadloos aan op onze kernwaarden en kent de volgende uitgangspunten:

- We stellen outcome ten behoeve van het publiek belang centraal
- We richten ons op de goede werking van het stelsel
- We werken probleem- en risicogericht
- We interveniëren responsief met de meest effectieve interventies
- We zijn in al ons handelen onafhankelijk, deskundig en betrouwbaar
- We kunnen daardoor reflectief zijn naar maatschappij en beleidsmakers

Het is onze maatschappelijke opgave om te zorgen voor een veilig verbonden Nederland, ook wanneer rollen en verantwoordelijkheden niet volledig gedefinieerd zijn. Vanuit deze wendbare en gezaghebbende positie nemen we hierin nu en in de toekomst onze verantwoordelijkheid. Het werk dat Agentschap Telecom verricht, raakt hiermee de hele samenleving.

Dit is een uitgave van:

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

agentschaptelecom.nl

T +31 (0)50 587 74 44

Voor een veilig verbonden Nederland

Januari 2022 | Publicatienr. 22400273