Digitale transitie: kansen en risico's

Cyberveiligheid, digitaal veilige apparatuur, kunstmatige intelligentie, telecomsecurity, 5G en frequentiemanagement zijn de grote thema's van vandaag en morgen. De Rijksinspectie Digitale Infrastructuur werkt aan een veilig verbonden Nederland.

Kansen en risico's
De Rijksinspectie Digitale Infrastructuur (de RDI) ziet een voortdurende grote dynamiek rond de digitale transitie. Die biedt *kansen* om onze welvaart te versterken en is ook een noodzakelijke voorwaarde voor de energietransitie. De digitale transitie brengt ook *risico's* met zich mee voor burgers en bedrijven in de Nederlandse samenleving. Zo maakt de toenemende afhankelijkheid van de digitale infrastructuur ons kwetsbaar voor uitval en verstoringen, bijvoorbeeld als gevolg van menselijke fouten en cyberaanvallen, mede tegen de achtergrond van de huidige geopolitieke situatie. Ook ontstaan er nieuwe maatschappelijke vraagstukken; denk aan de diverse dilemma's die aan artificiële intelligentie (AI) kleven.

Digitale infrastructuur is cruciaal voor het welslagen van de digitale transitie voor burgers en bedrijven. Om de risico's voor de samenleving te beperken zonder afbreuk te doen aan de kansen die de digitale transitie biedt, wordt op mondiaal en Europees niveau hard gewerkt aan noodzakelijke regulering voor betrouwbaarheid, integriteit en weerbaarheid van de digitale infrastructuur, zoals de NIS2-richtlijn, de Cyber Resilience Act en de AI-Act.

De RDI stelt, gelet op de kansen en risico's van de digitale transitie, een vijftal thema's centraal. Deze thema's zijn netwerksamenwerking, AI, digitale weerbaarheid, twin transition en de beschikbaarheid van een hoogwaardige digitale infrastructuur.

Netwerksamenwerking
Enerzijds kenmerkt de digitale transitie zich door een grote technologische complexiteit en een hoge snelheid waarmee innovaties als AI, kwantumtechnologie en blockchain hun toepassing vinden. Anderzijds voltrekt de digitale transitie zich in de volle breedte van economie en samenleving en houdt zich daarbij niet aan bestaande sectoren en structuren van de overheid en het toezicht. AI en kwantumtechnologie zijn bijvoorbeeld thema's die zich niet beperken tot één specifieke sector van de samenleving en overheid.

Om effectief te zijn voor de samenleving, is het voor het Nederlandse toezicht niet genoeg om enkel uit te blijven gaan van de traditionele sectorale benadering. Hoewel die sectorale benadering essentieel is (en blijft), ligt er een belangrijke veranderopgave in het verder uitbouwen van een effectieve netwerksamenwerking. Daarmee bundelen we krachten, versterken we elkaars inzet met ieders specifieke expertise en beperken we de toezichtslast op organisaties, bedrijven en instellingen.

AI
De ontwikkeling van AI gaat steeds sneller. Dit beïnvloedt ons leven en de maatschappij voortdurend. De impact van deze technologie op lange termijn is nog niet duidelijk. Om het gebruik van AI in goede banen te leiden moet bewaakt worden dat AI betrouwbaar en vertrouwenswaardig wordt toegepast in het digitale domein.

Om de risico's en de kansen verantwoord samen te laten gaan, wordt in Nederland samengewerkt met alle toezichthouders om het toezicht op AI vorm te geven. Samen met de Autoriteit Persoonsgegevens (AP)/Directie Coördinatie Algoritmes (DCA) werken we in 2024 aan het verder uitwerken van het toezicht op AI. Ook hier staat netwerksamenwerking op basis van sectorale expertise en bevoegdheden centraal.

Op basis van onze huidige toezichtstaken en die onder de AI-Act neemt de RDI het voortouw om duidelijkheid te geven in het verantwoord gebruik van AI, bijvoorbeeld door te werken aan standaardisatie.

Digitale weerbaarheid
Het is voor burgers en bedrijven in de digitale samenleving belangrijk dat de digitale infrastructuur veilig en betrouwbaar blijft. Maar we zien steeds vaker incidenten. De ene keer door bewuste aanvallen, zoals ransomware of DDOS. De andere keer door menselijke fouten of verkeerde risico-inschattingen. Een belangrijk risico – zeker tegen de achtergrond van de huidige geopolitieke situatie - is dat de digitale weerbaarheid van de vitale infrastructuur onder druk komt te staan. Door de digitale verknoping kan iedereen de gevolgen van een cyberincident direct ervaren als de integriteit of continuïteit van verschillende netwerken of systemen niet is gewaarborgd. Dit risico heeft grote impact op onze digitaliserende maatschappij omdat er een cascade effect kan plaatsvinden in verbonden ketens. Door ons toezicht vanuit de Europese Network & Information Systems (NIS)-regelgeving en onze centrale netwerkrol in Nederland mitigeren we samen de risico's.

Twin transition
Het huidige energiesysteem loopt tegen zijn grenzen aan. Dit zien we de laatste jaren steeds nadrukkelijker. Steeds meer burgers en bedrijven ondervinden hiervan hinder. De vraag naar het transport van elektriciteit kan bijvoorbeeld zo groot zijn dat de capaciteit van het elektriciteitsnet tekortschiet en dat leidt tot netcongestie. Onderdeel van de opgave is het decentraal (kunnen) opwekken en optimaal benutten van energie. Om die transitie naar een nieuw energiesysteem met verschillende hernieuwbare energiedragers te laten slagen, is digitalisering van cruciaal belang. Gezien deze samenhang tussen digitale transitie en energietransitie noemen we dit een *twin transition*.

Digitale oplossingen bieden bijvoorbeeld inzicht in het energiesysteem voor efficiënter energieverbruik, voor snelle aanbod- en vraagrespons, integratie en afstemming van verschillende energiedragers en helpen bij het optimaal ontwerpen van het toekomstig energiesysteem. Een gedigitaliseerd energiesysteem betekent echter ook nieuwe en andere risico's op uitval en storing voor burgers en bedrijven. Het aantal potentiële kwetsbaarheden neemt toe, met grotere gevolgen voor de beschikbaarheid en betrouwbaarheid van de (digitale) infrastructuur.

Beschikbaarheid van een hoogwaardige digitale infrastructuur
Een belangrijke grondstof voor de digitale transitie is het frequentiespectrum. Steeds meer innovatieve en waardevolle toepassingen voor de samenleving maken immers gebruik van draadloze verbindingen, bijvoorbeeld met 5G. Dit geeft druk op de beschikbaarheid van frequenties en leidt tot schaarste. Deze ontwikkeling vraagt om dynamischere vormen van spectrumallocatie en -gebruik. Tegelijkertijd legt de twin transition een steeds groter beslag op het gebruik van onze ondergrond: de aanleg van steeds meer kabels en leidingen brengt (veiligheids-)risico's met zich en daarmee de noodzaak tot verdergaande coördinatie.

Een gerelateerde ontwikkeling is het toenemende belang van veilig draadloos vitaal overheidsgebruik van kritische infrastructuur, gegeven de geopolitieke situatie en de impact daarvan op de nationale veiligheid; ook deze ontwikkeling noodzaakt tot meer coördinatie in het frequentiespectrum.

Ten slotte
Kortom, de digitale infrastructuur is de drager van de digitale transitie. De basis voor tal van ontwikkelingen, kansen, uitdagingen en bedreigingen en onlosmakelijk verbonden met ons dagelijks leven. Daarmee verdient de digitale infrastructuur een hoge plek op de politieke agenda en adequaat en effectief ingericht toezicht. Hoewel de Nederlandse

digitale infrastructuur al jarenlang internationaal vooroploopt, bestaat het risico dat deze voor lief genomen wordt. We moeten ons samen blijven inzetten om onze hoogwaardige digitale infrastructuur ook voor de toekomst te waarborgen en versterken zodat Nederland veilig verbonden blijft.