

Inbreng NLdigital aan de Ronde Tafel over de Nederlandse Digitaliseringsstrategie (NDS)

Inleiding

Met de presentatie van de Nederlandse Digitaliseringsstrategie (NDS) in juni 2025 heeft de overheid een belangrijke stap gezet richting een samenhangende digitale transformatie. De NDS benoemt zes prioriteiten: cloud, data, AI, burgergerichte dienstverlening, digitale weerbaarheid & autonomie en digitaal vakmanschap.

Als brancheorganisatie van de digitale sector onderschrijft NLdigital het belang van een nationale aanpak. Alleen al het proces van de totstandkoming waarbij niet alleen intern maar ook extern om input werd gevraagd is al positief. Dat creëert draagvlak in de buitenwereld en de behoefte om er een gezamenlijk succes van te maken. Tegelijkertijd vraagt de NDS ook om kritische reflectie: hoe effectief en toekomstgericht is de strategie, en onder welke voorwaarden kan zij daadwerkelijk slagen?

Algemene opmerkingen

Het huidige bredere kabinetsbeleid focust terecht op 'het pakken van de kansen die digitalisering biedt'. En dat is hoognodig, want Nederland loopt op allerlei vlakken achter waar het gaat om innovatie. De productiviteit is gestagneerd en dit tast ons toekomstig verdienvermogen aan. Zeker ook bij de (digitale) overheid is nog een wereld te winnen aan slimme inzet van digitale toepassingen. NLdigital heeft in haar [manifest richting de verkiezingen](#) gesteld dat Nederland moet digitaliseren of verarmen. Dat is geen loze kreet maar een harde realiteit. NLdigital hoopt dat de Tweede Kamer die urgentie ook voelt en niet alleen maar stil staat bij risico's en bedreigingen. Deze beperkte focus leidt er nu al toe dat overheden erg terughoudend zijn met de inzet van nieuwe technologie. Hierdoor blijft de potentie van digitale transformatie onderbelicht. Een voorbeeld hiervan is het werken in de cloud, dat aanzienlijke voordelen kent, terwijl de discussie zich voornamelijk toespitst op het aanscherpen van het inkoopbeleid voor clouddiensten. Ook de adoptie van kunstmatige intelligentie (zoals bepleit door de Sociaal-Economische Raad tijdens de Technische Briefing over het SER-advies *AI en werk*), cyberveiligheid en het versterken van digitale vaardigheden bij overheid, bedrijfsleven en burgers zijn van cruciaal belang. Deze investeringen zijn noodzakelijk om de kansen van digitalisering daadwerkelijk te verzilveren.

De komende jaren wordt binnen de overheid ook veel gevraagd van uitvoeringsorganisaties, zoals de Belastingdienst (inclusief de Dienst Toeslagen), UWV en SVB. Tegelijkertijd vormt het tekort aan uitvoeringscapaciteit een groeiend



knelpunt. Het Centraal Planbureau (CPB) berekende dat circa tien miljard euro aan kabinetsplannen mogelijk niet tot uitvoering komt als gevolg van capaciteitsproblemen (CPB, 2022a; 2022b).

Het rapport *Staat van de Uitvoering*, dat recentelijk is gepresenteerd, stelt dat naast complexe regelgeving vooral de gebrekkige gegevensuitwisseling tussen publieke dienstverleners het grootste knelpunt vormt. De centrale aanbeveling luidt dan ook: betrek de uitvoering bij het beleid. In 2023 rapporteerde PwC dat de gemiddelde arbeidsproductiviteit van grote uitvoeringsinstanties zoals UWV, de Belastingdienst en DUO aanzienlijk achterblijft ten opzichte van het nationale gemiddelde.

Dit perspectief komt momenteel onvoldoende tot uiting in beleidsdebatten en in de Nationale Digitaliseringsstrategie (NDS). Het verdient aanbeveling om in de verdere uitwerking van het beleid meer aandacht te besteden aan uitvoerbaarheid. Dit voorkomt dat beleidsvoornemens die in Den Haag worden ontwikkeld, in de praktijk niet realiseerbaar blijken. Positief geformuleerd: een herijking van het digitaliseringsbeleid kan bijdragen aan een betere dienstverlening aan burgers door overheidsinstanties. Hopelijk kan ook de Tweede Kamer hier aandacht aan besteden.

Sterke punten van de NDS

- Een aantal heldere prioriteiten: zes pijlers met focus op cloud, data en AI als systeemtechnologieën. Technologie wordt niet langer gezien als bedreiging maar juist als kans om beter en slimmer te werken.
- Doorbreken van versnippering: meer samenwerking binnen het Huis van Thorbecke is positief voor meer datagedreven werken binnen de overheid.
- Regie en governance: Thorbecketafel en NDS-Raad moeten doorzettingsmacht en draagvlak organiseren.
- Realistisch kijken naar autonomie en weerbaarheid: slim nadenken over digitale soevereiniteit en onafhankelijkheid.
- Meer kennis binnen de overheid over (de kansen met) digitalisering.

Kritische kanttekeningen

- Implementatierisico's: onduidelijkheid over budget, capaciteit en planning. Met het huidige demissionaire kabinet is het afwachten of er een budget wordt vrijgemaakt voor de NDS. Ook de kwaliteit van de vertaling naar een actiegericht programma zal beslissend zijn voor het succes van de NDS.
- Balans in de uitvoering: zorg dat de andere overheden en uitvoeringsorganisaties goed betrokken zijn. Dit voorkomt nieuw beleid dat niet uitvoerbaar blijkt.
- Rol van de markt nog onderbelicht: innovatiekracht bedrijfsleven blijft nog onvoldoende benut, kansen voor verduurzaming worden niet benoemd.

- Spanning centrale regie vs. federatief werken: centralere aansturing geeft risico op stroperigheid en onduidelijkheid.

Randvoorwaarden voor succes (voor NLdigital)

- Transparante investeringsagenda: helderheid over budget, capaciteit en prioritering. Zonder geld geen uitvoering van de visie. Sowieso zal veel afhangen van de doorvertaling naar een concrete actie agenda.
- Meetbare impact overheid: monitoring van positieve impact van NDS initiatieven op overheidsorganisaties in KPIs voor productiviteit, kostenbesparing en duurzaamheid.
- Meetbare burgerimpact: duidelijke doelen en benchmarks voor digitale dienstverlening.
- Echte publiek-private samenwerking: overheid als launching customer en structurele marktbetrokkenheid via de branche (NLdigital) en bredere coalities.
- Doorzettingsmacht en eenvoud in governance: duidelijke mandaten, minder bureaucratie.
- Lange termijn koers: het is te hopen dat een volgend kabinet deze agenda niet verlaat voor weer een nieuwe agenda.

Wat kan NLdigital bijdragen?

- Bruggen bouwen tussen overheid, bedrijfsleven en kennisinstellingen via consortia en samenwerking.
- Kennisdeling: Innovatie versnellen door pilots, sandboxes en best practices te delen.
- Meedenken over slimmer en effectiever aanbesteden door de overheid.
- Digitale vaardigheden versterken met opleidingsprogramma's en skills-initiatieven. De huidige samenwerking met RADIO kan worden opgeschaald.
- Signalen en feedback verzamelen en terugkoppelen naar NDS-Raad. Regulier overleg met de sector over de voortgang van de NDS.
- Maatschappelijke legitimiteit vergroten door leden te stimuleren tot ethisch en inclusief innoveren.

Conclusie

De NDS biedt een belangrijk kader voor de digitalisering van Nederland, maar kent kwetsbaarheden: te veel focus op techniek, onvoldoende meetbaar en een te beperkte rol voor de markt. Voor succes zijn een investeringsagenda, nauwe samenwerking met andere overheden en uitvoeringsorganisaties, meetbare doelen en een betrokken markt noodzakelijk.

NLdigital kan, als representant van de digitale sector, een onmisbare partner zijn bij

de uitvoering van de NDS. Door bruggen te slaan, innovatie te versnellen en maatschappelijke waarden te borgen, kan NLdigital bijdragen aan een strategie die niet alleen overheidsgericht is, maar daadwerkelijk de samenleving en economie verder brengt.

Specifieke inbreng voor de Ronde Tafel Blok 2 (15:00 – 16:00 uur): Aanbieders en beschermers van digitale dienstverlening

Welke cyberveiligheidsrisico's kleven er aan strategische afhankelijkheden?

De aard en omvang van de cyberveiligheidsrisico's die gepaard gaan met strategische afhankelijkheden zijn sterk afhankelijk van de wijze waarop deze afhankelijkheden zijn ingericht. In de praktijk is vrijwel iedere organisatie in zekere mate afhankelijk van IT-leveranciers, ongeacht of de dienstverlening intern wordt georganiseerd of is uitbesteed. Deze afhankelijkheid vereist een strategische benadering. Daarbij moet worden opgemerkt dat afhankelijkheid van één leverancier altijd ongewenst is, ongeacht waar deze vandaan komt.

Het is van belang dat organisaties expliciet stilstaan bij de onzekerheden die dergelijke afhankelijkheden met zich meebrengen. Dit omvat onder meer het opstellen van noodscenario's en het treffen van passende voorzorgsmaatregelen. Het uitvoeren van gedegen risicoanalyses en het implementeren van mitigerende maatregelen wordt dan ook nadrukkelijk aanbevolen. De specifieke risico's, de wijze van omgang daarmee en de te nemen maatregelen verschillen per organisatie. In algemene zin geldt echter dat het structureel omgaan met risico's – en daarmee ook met afhankelijkheden – een integraal onderdeel zou moeten vormen van het cybersecuritybeleid.

Daarnaast dient te worden onderkend dat geen enkel scenario volledig risicoloos is. Systemen die door grote aantallen gebruikers worden benut, vormen een aantrekkelijk doelwit voor kwaadwillenden. Tegelijkertijd zijn dergelijke systemen doorgaans beter beveiligd, juist vanwege de continue blootstelling aan dreigingen.

Welke afhankelijkheden ziet u momenteel als grootste kwetsbaarheid in de digitale infrastructuur van Nederland?

In dit verband verwijzen wij graag naar het rapport [“Van kwetsbaar naar weerbaar”](#) van ABDTOPConsult, opgesteld in opdracht van de Algemene Bestuursdienst en [recent gedeeld met de Tweede Kamer](#) door de minister van Binnenlandse Zaken en Koninkrijksrelaties. Dit rapport onderstreept terecht het belang van het beschikken over uitwijk- en terugvalmogelijkheden.

Binnen de sector wordt dit rapport gezien als een kans om in samenwerking met de overheid te werken aan een meer gediversifieerd en robuust IT-landschap. Het is van belang dat de rijksoverheid meer grip verkrijgt op de digitale infrastructuur, haar kennispositie versterkt en ervoor zorgt dat voor iedere strategische afhankelijkheid adequate alternatieven beschikbaar zijn.

Is de Nederlandse ICT-sector nu in staat om cyberveilige infrastructuur en applicaties te leveren?

De Nederlandse ICT-sector beschikt over de capaciteit om op grote schaal cyberveilige infrastructuur en applicaties te leveren. Recente gebeurtenissen, zoals de verhoogde internationale aandacht tijdens de NAVO-top, zijn op het gebied van cybersecurity goed doorstaan. Hoewel er nog aanzienlijke verbeteringen mogelijk zijn, is er sprake van een positieve ontwikkeling.

De sector is actief betrokken bij het versterken van de digitale weerbaarheid en levert reeds op grote schaal diensten in het kader van de aankomende Cyberbeveiligingswet (NIS2). Er is sprake van een duidelijke bereidheid en inzet om verdere verbeteringen te realiseren.

Draagt het zwaar(der) meewegen van autonomie in de risicobeoordeling bij aanbestedingen van het Rijk bij aan de digitale weerbaarheid van Nederland?

Het begrip autonomie dient in dit verband zorgvuldig te worden gedefinieerd. Autonomie verwijst naar het beschikken over voldoende controle en zeggenschap over hard- en software, teneinde zelfstandig en onafhankelijk besluiten te kunnen nemen.

Het zwaarder laten meewegen van autonomie in risicobeoordelingen in deze zin is verstandig. Dit impliceert onder meer investeringen in uitwijk- en terugvalmogelijkheden, evenals in de opbouw van interne kennis binnen de overheid. Daarnaast vereist het het maken van bewuste technologische keuzes en het hanteren van uitwisselbare standaarden. Deze uitgangspunten worden breed onderschreven binnen de sector. De dieper liggende discussie gaat eigenlijk over het onderwerp leveranciersafhankelijkheid. Het gaat eigenlijk meer om goed opdrachtgeverschap, waarbij vooraf met de leverancier goede afspraken gemaakt moeten worden over een exit-strategie, dataportabiliteit, interoperabiliteit en open standaarden. Daarmee kan de afhankelijkheid van één leverancier, los van waar die leverancier vandaan komt, worden voorkomen.