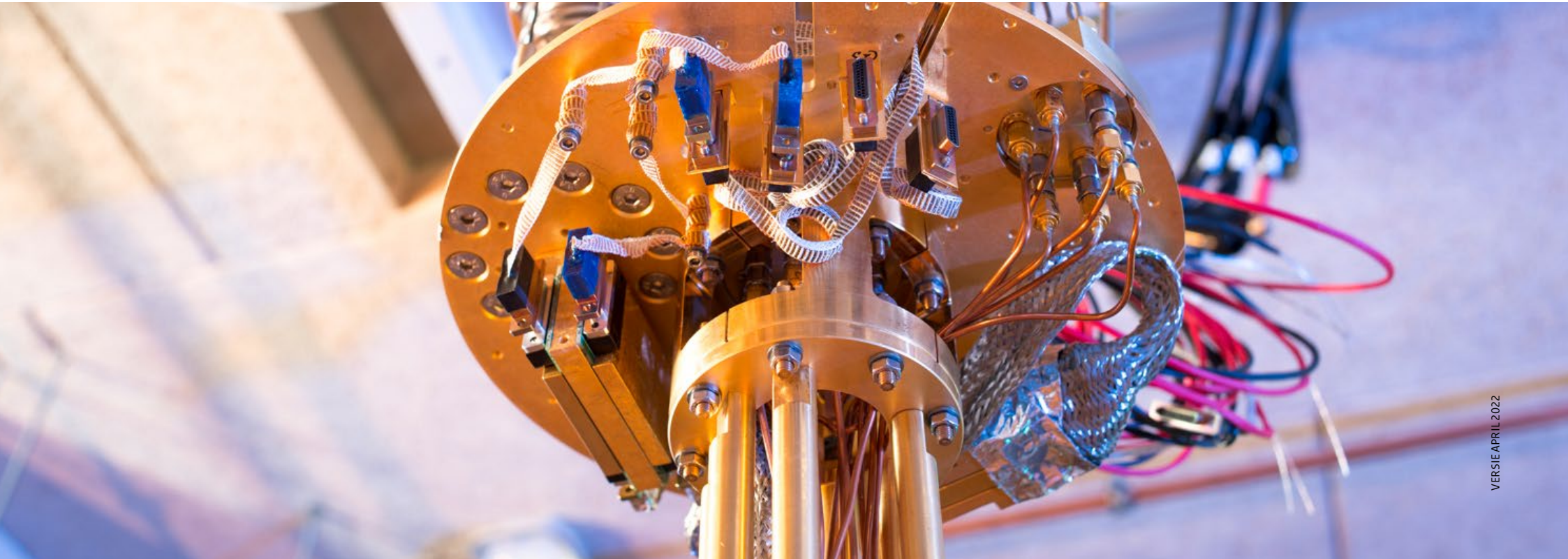




TechAgenda

Technologische ontwikkelingen met impact op Recht, Veiligheid en Migratie



Colofon

De Technologieagenda van het Ministerie van Justitie en Veiligheid biedt inzicht in de relevante technologieën voor het ministerie in de komende jaren. De agenda is tot stand gekomen met medewerking van velen binnen en buiten het ministerie van Justitie en Veiligheid. De Directie Innovatie, Kennis en Strategie heeft dit proces gefaciliteerd.

Fotografie

Mark David (cover), Tineke Dijkstra (p. 4), Paul Voorham (p. 9),
Louis Ottens (p. 10), Edwin Walvisch (p. 28)

Illustraties

Flatland

Directie X

Technologieprogramma
V1.0

April 2022

Inhoud

1	Managementsamenvatting	3
2	Inleiding	4
	2.1 Aanleiding	5
	2.2 Doel	5
	2.3 Aanpak	8
3	Relevante technologieën in beeld	9
	3.1 Digitale veiligheid	12
	3.2 Artificiële intelligentie	14
	3.3 Data science	16
	3.4 Netwerken en infrastructuur	18
	3.5 Digitale werkelijkheid	20
	3.6 Quantum	22
	3.7 Life science technologies	24
	3.8 Engineering technologies	26
4	Handelingsperspectief voor het technologie-portfolio	28
	4.1 Acteren in verschillende vormen en intensiteiten	29
	4.2 Opschalen: van ‘ontwikkelen’ naar ‘realiseren’	31
	4.3 Monitoring en sturing	32
	Bijlage: Gevolgd proces	33
	1. Een basislijst voor de Rijksoverheid	33
	2. De long list voor JenV	35
	3. Samenhang in clusters	37
	4. Koppeling met het Organisational readiness level (ORL)	41
	5. Lessons Learned	45

1 Managementsamenvatting

In de afgelopen periode is een overzicht opgesteld van de relevante technologieën voor het ministerie van Justitie en Veiligheid (JenV). ‘Relevante technologieën’ betekent hier dat deze technologieën:

- ofwel tot kansen of risico’s voor de maatschappij kunnen leiden (in relatie tot bijvoorbeeld burgerrechten, veiligheid, maatschappelijke en ethische aspecten),
- ofwel dat de technologieën tot kansen of risico’s kunnen leiden voor een efficiënte of effectieve taakuitoefening van JenV-organisaties.

Het overzicht van relevante technologieën is tot stand gekomen in een proces waarbij de ‘binnenwereld’ van JenV en haar uitvoeringsorganisaties, en de grotere wereld buiten JenV betrokken is geweest.

Technologieën zijn in de breedte geanalyseerd en vervolgens geprioriteerd aan de hand van de verwachte impact en urgentie voor JenV. Hierna zijn 6 clusters aangebracht met groepen technologieën die het meest van belang zijn voor de breedte van JenV. In deze publicatie wordt ieder cluster en iedere technologie kort omschreven, met belangrijke kansen en risico’s voor JenV.

 1. Digitale veiligheid

 2. Artificiële intelligentie

 3. Data science

 4. Netwerken en infrastructuur

 5. Digitale werkelijkheid

 6. Quantum

 7. Life Science Technologieën

 8. Engineering Technologieën

De 6 clusters zijn aangevuld met twee clusters technologieën die voor een specifiek deel van JenV van belang zijn. Dit zijn Life Science Technologieën en Engineering Technologieën. Alle clusters en technologieën worden in hoofdstuk 3 toegelicht.

Met behulp van het overzicht in deze Technologieagenda (kort: TechAgenda) kan JenV pro-actief acteren om risico’s te beheersen en kansen te grijpen. Concreet betekent dit onder andere:

- Prioriteiten stellen en inzet bepalen ten behoeve van kennisontwikkeling bij kennisinstellingen over technologie en innovatie en bevorderen dat de ontwikkelde kennis over technologie aansluit op beleid en uitvoering.
- Capaciteit en middelen (investeringen) richten voor beleidsontwikkeling, onderzoek en experimenten.
- De betekenis van technologie voor de beleidsdomeinen en taakvelden van JenV verder verdiepen.

Welk handelingsperspectief voor JenV wenselijk is, verschilt per technologie. Dit is afhankelijk van de volwassenheid en de praktische toepasbaarheid van de technologie, en van de mate waarin JenV al voorbereid is op deze technologie. Op deze aspecten is voortdurend ontwikkeling.

Deze TechAgenda vormt het uitgangspunt voor het verder versterken van de samenwerking op het gebied van technologiebeleid binnen en buiten JenV. Door samen te werken over domeinen en organisaties heen en optimaal gebruik te maken van elkaars kennis, analyses en scans, kunnen we kennis over (gebruik van) technologie vergroten. Steeds met het doel tijdig te acteren op technologische ontwikkelingen die zich aandienen.



2

Inleiding

Voor u ligt de Technologieagenda (kort: TechAgenda) van het ministerie van Justitie en Veiligheid (JenV). Deze publicatie is tot stand gekomen op basis van deskresearch en consultatie van beleidsmedewerkers, uitvoeringsorganisaties, kennispartners, technologie-experts en wetenschapsjournalisten, zowel van binnen als buiten het ministerie. In een gezamenlijk proces is in kaart gebracht welke relevante technologische ontwikkelingen er aan komen, en welke impact verwacht kan worden op de maatschappij en op JenV.

2.1 Aanleiding

De maatschappelijke opdracht van JenV is om de rechtsstaat goed te laten werken, Nederland veiliger te maken en een rechtvaardig migratiebeleid te ontwikkelen en uit te voeren. Dit doen we in een snel veranderende samenleving. Ontwikkelingen als internationalisering, digitalisering, polarisering en veranderende verwachtingen over de overheid hebben grote impact op het werk van JenV-ambtenaren.

Veel maatschappelijke ontwikkelingen worden beïnvloed door technologische ontwikkelingen, zoals de digitalisering van criminaliteit. Dat heeft ook weerslag op de opgaven van JenV. Technologieën, zoals onder andere artificiële intelligentie, immersieve technologie en -op termijn- quantumtechnologie, bieden kansen en leveren uitdagingen en risico's op.

JenV wil adequaat en structureel aansluiten op technologische ontwikkeling van vandaag, morgen en overmorgen:

- Omdat JenV burgers en bedrijven wil beschermen en, indien nodig, wil reguleren wanneer nieuwe technologieën risico's en ethische, juridische en maatschappelijke vraagstukken met zich meebrengen.
- En om zelf op verantwoorde wijze technologie in te kunnen zetten om het JenV-werk beter (effectiever, efficiënter) te doen en de maatschappelijke doelen te bereiken.

De wens om aan te sluiten en zelfs richtinggevend te zijn wordt versterkt door de toenemende aandacht voor effecten van technologie in de Europese en Nationale politiek. De vaste Kamercommissie Digitale Zaken en de nieuwe staatssecretaris Digitalisering zijn hier voorbeelden van. Vanuit de Europese Commissie is met onder andere de recente Digital Market- en Services Act, en met de AI verordening gekozen voor een sterkere betrokkenheid bij technologische ontwikkelingen.

2.2 Doel

Deze TechAgenda geeft zicht op wat de belangrijke technologieën¹ voor JenV zijn in de komende jaren, zodat zij haar prioriteiten hierop kan richten, en beter kan worden in de omgang met nieuwe technologieën². De TechAgenda geeft richting aan het gesprek over technologie binnen JenV en faciliteert samenwerking binnen en tussen JenV-organisaties, en met bedrijven en kennisinstellingen. Daar waar keuzes te maken vallen, kan met behulp van de TechAgenda beredeneerd voorrang gegeven worden aan bepaalde technologieën.

Dit moet er onder andere toe leiden dat:

- Beleidsmakers en wetgevingsjuristen vroegtijdig en pro-actief nieuwe vraagstukken/risico's kunnen signaleren op het vlak van beleid- en wetgeving.
- Beleidsmakers kamervragen rond technologische onderwerpen eenvoudig kunnen afdoen, en snel kunnen zien waar technologische ontwikkelingen en innovatie kunnen worden ingezet ten behoeve van de maatschappelijke opgaven.
- Wetgevingsjuristen met minder moeite toekomstvaste wetgeving kunnen produceren.
- Innovatoren meer gebruik kunnen maken van de leerervaringen van andere (JenV-)organisaties.
- Kenniscoördinatoren goede vragenstellingen aangeleverd kunnen krijgen voor het richten van onderzoek door kennispartners.
- Beslissers hun organisatieonderdeel goed kunnen laten inspelen op de uitdagingen van morgen.

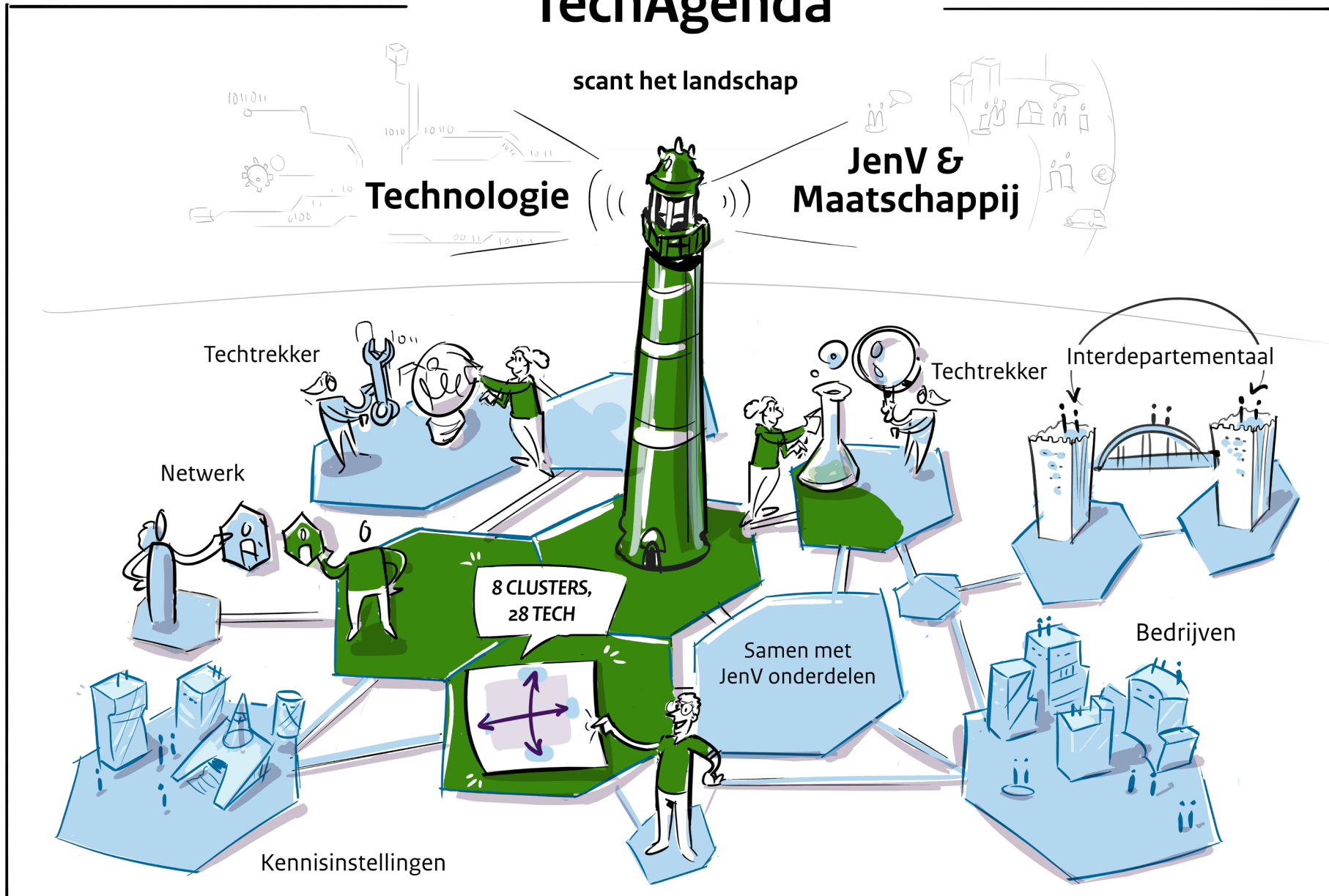
¹ De TechAgenda gebruikt de term technologieën. Het betreft echter zowel technologieën; technologische ontwikkelingen en in een enkel geval een (technologisch) concept of een dienst. Voor de leesbaarheid wordt zoveel mogelijk de term technologieën gebruikt.

² Zie de Whitepaper 'Focus op technologie' op www.innoveermeemetjenv.nl/technologie

Buiten de muren van het ministerie, in de maatschappij, wordt de echte waarde geleverd met een JenV dat goed aansluit op technologische ontwikkelingen en tijdig acteert:

- Burgers kunnen hun contacten met de overheid ervaren als veilig en rechtvaardig.
- Burgers hopen dat Nederland een veilig en rechtvaardig land blijft, ook als de maatschappij zo snel verandert. Ze kijken daarvoor onder andere naar de overheid.
- Kennisinstanties kunnen toegevoegde waarde leveren met hun technologieonderzoek, en hun resultaten goed laten landen binnen JenV-organisaties.
- Bedrijven krijgen investeringszekerheid door consistent beleid om producten en diensten te ontwikkelen en vermarkten.

TechAgenda



Figuur 1.1: Overzicht en samenwerking TechAgenda: In de figuur is het technologielandchap waar JenV zich in beweegt zichtbaar. De TechAgenda fungeert als vuurtoren die overzicht biedt in het landschap en richting geeft aan besluitvorming rondom technologische ontwikkeling.

2.3 Aanpak

Uitgaande van de technologiescan van JenV uit 2018 en de rijksbrede Technologiescan uit 2020³, zijn bijna 60 technologieën geïdentificeerd met een relevantie voor de Rijksoverheid en voor JenV. Deze informatie is aangevuld en gevalideerd aan de hand van beschikbare onderzoeken, rapporten en gesprekken met experts.

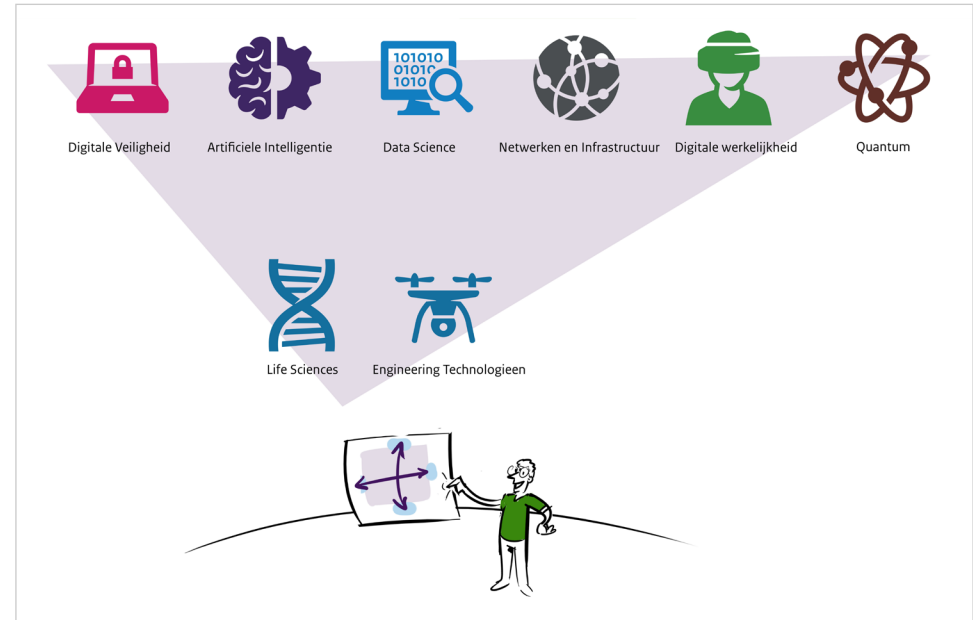
Samen met beleidsmedewerkers, uitvoeringsorganisaties, kennispartners, technologie-trekkers en enkele wetenschapsjournalisten is, op basis van de zogenaamde Delphi methode, in kaart gebracht welke technologieën voor JenV relevant zijn, en welke impact verwacht kan worden op de maatschappij en op het ministerie. Dit heeft geleid tot een selectie van 28 technologieën met de grootste impact en/of urgentie voor JenV. Deze lijst is in workshops en sessies besproken en geëvalueerd met betrokkenen van binnen en buiten JenV.

Het doel van de gekozen aanpak was uitdrukkelijk niet om een lijst te maken waarbij de ene technologie als belangrijker wordt geduid dan een andere, maar om de organisatie richting te geven bij het maken van beslissingen op het gebied van inzet van capaciteit en middelen. Een schikking van deze technologieën in clusters is daarvoor van belang.

Dit heeft geresulteerd in 6 clusters die voor heel JenV relevant zijn, aangevuld met twee clusters met 'specials' die voor een specifiek domein of taakveld (zeer) relevant zijn.

Een aantal clusters, zoals bijvoorbeeld artificiële intelligentie en data science, ligt dicht tegen elkaar aan. Kijkend naar kansen, risico's en handelingsperspectief, zijn ze wel in twee clusters gesplitst. In de beschrijving van elk cluster zijn de overwegingen die aan de clustering ten grondslag liggen toegelicht. In de bijlage is het doorlopen proces nader toegelicht.

Hoofdstuk 3 beschrijft deze clusters van technologieën en hun relevantie voor JenV. In hoofdstuk 4 wordt ingegaan op het handelingsperspectief voor JenV.



Figuur 1.2: Clusters van technologieën

³ De scan is opgesteld door de interdepartementale werkgroep technologieverkenningen (WGTV) van de Rijks Innovatie Community. In dit netwerk van technologieverkenners van diverse departementen en grote uitvoeringsorganisaties wordt samengewerkt om technologische ontwikkelingen te volgen en te duiden. Zie www.techfocus.nl



3

Relevante technologieën in beeld

Veel maatschappelijke ontwikkelingen worden beïnvloed door technologie, en dat heeft ook weerslag op de opgaven van JenV. Deze constatering komt al een aantal jaar in het Strategisch Omgevingsbeeld van JenV⁴ naar voren. Het Omgevingsbeeld signaleert onder andere de toenemende afhankelijkheid van het digitale domein en verschuivingen in criminaliteit naar het digitale domein. Maar ook het meer op de voorgrond komen (en makkelijker verspreiden) van extremistische ideeën en de toename van mogelijkheden om op afstand samen te werken en te ontspannen. Het Omgevingsbeeld geeft daarbij inzicht in actuele trends ; de TechAgenda geeft zicht op relevante technologieën voor vandaag, morgen en overmorgen.

⁴ Strategisch Omgevingsbeeld 2021 - Maatschappelijke ontwikkelingen compact in beeld | Nieuwsbericht | [Rijksoverheid.nl](https://rijksoverheid.nl)



De TechAgenda geeft inzicht in de technologieën die op komst zijn en impact hebben op de maatschappelijke opgaven van JenV, zoals die onder meer in de hoofdlijnennotitie JenV⁵, en in het coalitieakkoord⁶ benoemd zijn. Denk bijvoorbeeld aan de opgave van een sterke en toekomstbestendige rechtstaat of de aanpak ondermijning. Ook in de kamerbrief⁷ over de hoofdlijnen van het beleid van de staatssecretaris van Digitalisering komt dit naar voren. Digitalisering komt naar voren dat de opgave om digitalisering in goede banen te leiden groot is.

Aan de hand van verwachte *impact* op het werkveld van JenV en op de maatschappij en de inschatting van de *urgentie* voor JenV zijn 28 technologieën geprioriteerd. Technologie is hierbij een breed gebruikte term. Op de lijst zijn zowel technologieën en technologische ontwikkelingen opgenomen die duidelijk toepassingsgericht zijn (zoals beeldherkenning, spraaktechnologie), technologieën die meer als technisch fundament dienen (blockchain of big data) en in een enkel geval een op technologie gebaseerd concept of dienst (zoals sociale media). Deze zijn naast elkaar terug te vinden in de TechAgenda op basis van hun relevantie voor JenV.

Aan de hand van verwachte impact op het werkveld van JenV en op de maatschappij en de inschatting van de urgentie voor JenV, zijn 28 technologieën geprioriteerd.

5 Hoofdlijnenbrief Justitie en Veiligheid | [Rijksoverheid.nl](https://rijksoverheid.nl)

6 Coalitieakkoord 2021-2025 | [Rijksoverheid.nl](https://rijksoverheid.nl)

7 Kamerbrief hoofdlijnen beleid voor digitalisering | Kamerstuk | [Rijksoverheid.nl](https://rijksoverheid.nl)

Tabel 3.1: Clusters voor JenV

Clusters TechAgenda		Technologie
 1. Digitale veiligheid	Technologieën met impact op de veiligheid van digitalisering, gegevensuitwisseling, communicatie, identificatie, dataopslag en gebruik van netwerken en infrastructuur	Digital ID en self-sovereign identity Post-Quantum Cryptografie/PQC Digital security en cybersecurity Privacy enhancing technologieën Blockchain
 2. Artificiële intelligentie	Technologieën die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken.	Synthetic media Beeldherkenning Predictieve analyse Profiling Natural language processing Beslisalgoritmes en expertsystemen
 3. Data science	Technologieën waarbij veel data verzameld en/of geanalyseerd worden. Ten opzichte van het cluster artificiële intelligentie ligt de focus bij data science minder op intelligent gedrag van de systemen.	Social media en social media analytics Big data en data analytics incl. Datavisualisatie Imaging technologieën incl. camera, infrarood, radar, WAMI Robotic Process Automation (RPA)
 4. Netwerken en Infrastructuur	Technologieën die bijdragen aan noodzakelijke verbindingen voor verdergaande digitalisering. De technologieën in dit cluster zijn daarmee randvoorwaardelijk voor veel andere ontwikkelingen	Internet of things Satellieten incl. Low Earth Orbit 5G Cloud en high performance grid computing
 5. Digitale werkelijkheid	Technologieën die bijdragen aan een digitale omgeving waarin men leeft, werkt of ontspanning zoekt, en waarin veiligheid, privacy en recht aandacht vereisen. Denk aan de Metaverse. Digitale werkelijkheid heeft directe relatie met artificiële intelligentie en sociale media	Virtual reality, Augmented reality Wearables Digital twin
 6. Quantum	Technologieën die gebruik maken van eigenschappen uit de quantummechanica. Dit cluster omvat specifiek de ontwikkeling van de sleuteltechnologie 'Quantum' (-computing, -communicatie en -sensoren)	Quantum computing en communicatie Quantum sensoren en metrologie
Specials TechAgenda		Technologie
 7. Life sciences	Technologieën die gebaseerd zijn op of gebruik maken van menselijk materialen en organen	DNA-analyse Biochips Genetic Engineering
 8. Engineering technologies	Technologieën met een fysieke verschijningsvorm. Robots, drones, autonome voertuigen en vaartuigen	Robots Autonomous vehicles & systems



3.1 Digitale veiligheid

Het cluster Digitale veiligheid bundelt een aantal technologieën die cruciaal zijn in het licht van de veiligheid van de digitaliserende maatschappij. Dit betreft verschillende technologieën die impact hebben op de veiligheid van gegevensuitwisseling, communicatie, identificatie, dataopslag en gebruik van netwerken en infrastructuur.

Digital Security en cybersecurity omvat technologieën met betrekking tot het beschermen van computers, servers, mobiele apparaten, elektronische systemen, netwerken en gegevens tegen cyberaanvallen.

Post-Quantum Cryptografie omvat nieuwe manieren van versleuteling met behulp van Quantum sleutels die ook na de komst van quantumtechnologie nog veiligheid bieden.

Privacyenhancing technologies (PETs), selfsovereign identity (SSI) en smart contracts zijn toepassingen die onder andere gebruik maken van concepten uit de blockchain technologie. Ze worden ontwikkeld om op nieuwe manieren veilig gegevens uit te kunnen wisselen of een eigen identiteit, eigendom of contracten te kunnen beheren. Deze ontwikkelingen dragen daarmee bij aan een digitale veilige en rechtmatige maatschappij.

Blockchain is een concept dat niet uitgaat van centrale servers en databases, maar juist van gedistribueerde ontwerpen. Bij de technologie Blockchain is niet één vertrouwde partij leidend, maar een netwerk. De cryptovaluta 'Bitcoin' is een van de bekendste voorbeelden van een blockchain-toepassing, naast bovengenoemde ontwikkelingen.

Relevantie voor JenV

Digitale veiligheid is zeer relevant voor JenV, zowel vanuit het maatschappelijk belang als uit het belang van de bedrijfsvoering van JenV-organisaties zelf. Dit maatschappelijk belang van een digitaal veilig Nederland kan niet onderschat worden. Onze afhankelijkheid van digitale diensten is enorm toegenomen⁸, en daarmee onze kwetsbaarheid voor datalekken en hacks.

Naast beveiliging van vitale infrastructuur, burgers en bedrijven, hebben JenV-organisaties ook een groot belang in het beveiligen van de eigen informatiesystemen tegen inbreuken. Veilige informatie-uitwisseling tussen partijen is relevant bij onder andere het bestrijden van ondermijnende criminaliteit.

Tenslotte komt het belang van dit cluster ook voort uit de beleidsmatige verantwoordelijkheid voor privacy en rechtvaardigheid: Met name *self-sovereign identities* en *privacy enhancing technologies* zijn in dat kader relevant.

Onze afhankelijkheid van digitale diensten is enorm toegenomen, en daarmee onze kwetsbaarheid voor datalekken en hacks.

⁸ Cybersecuritybeeld Nederland 2021 | NCTV publicaties | nccsc.nl



3.1 Digitale veiligheid (vervolg)

Kansen en risico's voor beleid en uitvoering

Digitale veiligheid is voortdurend in het geding. In het domein van digital security en cyber-security worden steeds meer geavanceerde technologieën ontwikkeld. Hiermee kunnen digitale infrastructuren en gegevens worden aangevallen, maar kan ook beschermd worden tegen aanvallen. Voorbeelden zijn onder andere: Automated vulnerability scanning en Automated response. Op dit gebied is binnen JenV veel kennis en expertise beschikbaar bij de NCTV en het NCSC. Belangrijk is dat de door hen ontwikkelde technieken ook hun weg vinden naar toepassing binnen JenV.

Van quantumcomputers wordt verwacht dat deze over zo'n 10 jaar in staat zijn om de huidige encryptiestandaarden te doorbreken. Hierdoor zijn bestanden en berichten anno 2022 al niet meer veilig tegen aanvallen van het type *store and decrypt later*. Bedrijfsgeheime of privacygevoelige informatie van nu ligt straks op straat. Nieuwe Post-Quantum Cryptografiestandaarden dienen zich aan om dit probleem te ondervangen. Deze zullen door de JenV-organisaties moeten worden geïmplementeerd.

Veel digitale diensten van marktpartijen én overheid maken gebruik van *digitale identiteiten* zoals DigID of eHerkenning. Daarmee weten dienstverleners met wie ze zaken doen. Het gedachtegoed van SSI is erop gebaseerd dat individuen controle en zelfbeschikking zouden moeten hebben over hun digitale identiteit en de gegevens die deze identiteit vormen. De Europese Commissie heeft een raamwerk voor SSI ontwikkeld dat volgens planning in 2022-2023 tot SSI-oplossingen gaat leiden.

Kansen voor online identiteitsmanagement liggen onder andere in het tegengaan van lekken van persoonlijke gegevens en wachtwoorden en het stroomlijnen van administratieve processen, zodat burgers minder vaak hun gegevens hoeven invoeren.

Risico's van SSI-toepassingen liggen onder andere in de langere termijn: stimuleren digitale identiteiten en SSI-toepassingen niet juist een controle-maatschappij?

Privacy Enhancing Technologies (PET's) maken het mogelijk om data tegelijkertijd te benutten en te beschermen. In het bijzonder bieden PETs kansen voor JenV, omdat JenV verantwoordelijkheid draagt voor de bescherming van privacy en persoonsgegevens, zoals vastgelegd in de AVG. Privacybescherming wordt sterk uitgedaagd door technologische ontwikkelingen op het terrein van data-analytics, artificiële intelligentie, DNA-technieken en gezichtsherkenning. Met PETs worden technologische mogelijkheden ingezet om persoonsgegevens en privacy te beschermen. PETs geven invulling aan de principes van privacy-by-design. JenV is goed voorgesorteerd op de ontwikkeling van PET⁹ en het licht voor de hand de kansen die PET biedt verder uit te bouwen en te benutten.

⁹ Snel, slim en privacyvriendelijk gegevens uitwisselen met Ma3tch | magazines.rijksoverheid.nl/jenv/jenvmagazine en Winnaars Nederlandse Privacy Awards 2021 | privacyawards.nl



3.2 Artificiële intelligentie

Artificiële intelligentie (AI) kent verschillende definities. Het precies definiëren van AI is lastig: de term ‘algoritmes’ is te breed, maar een afbakening op *machine learning*, en *deep learning* is weer te smal. JenV gebruikt de definitie uit het strategisch actieplan voor artificiële intelligentie (2019) van het ministerie van Economische zaken en klimaat: “AI verwijst naar systemen die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken”. Dit is ook de omschrijving van AI zoals die wordt gebruikt door de Europese Commissie.

AI-toepassingen maken al sinds enige tijd onderdeel uit van ons dagelijks leven. Denk bijvoorbeeld aan intelligente zoekmachines, aan rij-ondersteuning in auto’s en aan aanbevelingsalgoritmen bij video-on-demand diensten.

Relevantie voor JenV

Het overgrote deel van bedrijven in Nederland (86 procent¹⁰) voorziet dat AI een grote impact gaat hebben binnen hun sector. Het kabinet beschouwt AI dan ook als een zogenaamde ‘sleuteltechnologie’, die veel maatschappelijke en economische kansen biedt¹¹. De Nederlandse en Europese overheid investeren fors in onderzoek en ontwikkeling, net als het bedrijfsleven. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) vergelijkt AI als een ‘systeemtechnologie’ met elektriciteit, de verbrandingsmotor en de komst van de computer¹². Het coalitieakkoord 2021 is ambitieus ten aanzien van de rol van Nederland voor de mensgerichte inzet van artificiële intelligentie.

De relevantie voor JenV komt enerzijds voort uit de rol die JenV heeft in het waarborgen van publieke waarden als rechtvaardigheid en privacy bij maatschappelijke toepassingen van AI. Het juridisch kader hieromheen is volop in ontwikkeling. Anderzijds maken de veiligheidsrisico’s AI als cluster ook relevant voor JenV. De technologie biedt ook kwaad-

willenden nieuwe mogelijkheden. AI biedt JenV kansen om maatschappelijke opgaven beter en sneller op te pakken. Denk aan het verbeteren van de capaciteitsplanning in de strafrecht- of migratieketen, het sneller signaleren van cyberdreigingen of een adequatere behandeling van WOB-verzoeken of Kamervragen. Tenslotte biedt AI ook kansen voor het optimaliseren van allerlei arbeidsintensieve JenV-processen als analyses, vertalingen en controles. Daarbij is ook duidelijk dat er politiek veel aandacht is voor de transparante, verantwoorde toepassing van AI-algoritmes. Zeker in het overheidsdomein.

Vanwege de hoge impact en urgentie, heeft JenV een speciaal AI-team in het leven geroepen, dat begin 2022 de AI-strategie voor JenV¹³ opleverde.

Kansen en risico’s voor beleid en uitvoering

In JenV’s eigen AI-strategie worden allerlei kansrijke toepassingen van AI geschetst, zoals toepassingen van *tekstherkenning* om binnengekomen stukken op thema te sorteren bij het CJIB, het doorzoeken van grote hoeveelheden digitale sporen bij politie/NFI. En *beeldherkenning* om documentfraude te kunnen herkennen bij IND.

Spraakherkenning of Natural language processing biedt ook veel kansen voor al die situaties waarin JenV-ambtenaren gesproken tekst omzetten in geschreven tekst. Denk aan verhoren, verslagen van vergaderingen en vertalingen. Het correct geautomatiseerd verwerken van persoonsgegevens vergt daarbij speciale aandacht.

Beslisalgoritmes en expertsystemen bieden kansen voor situaties waarin snel relevante kennis beschikbaar moet komen, zoals in crisissituaties. Of situaties waarin specialistische kennis ingezet moet worden, bijvoorbeeld bij dossiervoorbereiding ten behoeve van rechtspraak. Expertsystemen kunnen een gelijke beoordeling in gelijkwaardige gevallen ondersteunen (belangrijk voor rechtsgelijkheid) en kunnen bij besluitvoering worden ingezet om verschillende alternatieven (tegenspraak) te tonen en daarmee het risico op tunnelvisie te verkleinen.

¹⁰ Strategisch Actieplan voor Artificiële Intelligentie | [Rijksoverheid.nl](https://rijksoverheid.nl)

¹¹ Nederlandse Digitaliseringsstrategie 2020 | [Rijksoverheid.nl](https://rijksoverheid.nl)

¹² WRR: Opgave AI. De nieuwe systeemtechnologie | wrr.nl

¹³ De AI strategie van JenV is in januari 2022 vastgesteld en wordt binnenkort gepubliceerd.

Meer informatie via AI@minjenv.nl



3.2 Artificiële intelligentie (vervolg)

Risico's

AI-algoritmen zijn vaak complex, en komen vaak geheel of gedeeltelijk tot stand in een leerproces op basis van aangeleverde data. Transparantie, controleerbaarheid en uitlegbaarheid zijn daarom cruciale begrippen bij het gebruik van AI algoritmes. Het is op voorhand niet altijd duidelijk welke acties of 'beslissingen' een algoritme neemt, en op basis waarvan dat precies gebeurt (transparantie). Bij traditionele algoritmen is dat meestal wel het geval. Een andere zorg bij AI-algoritmen ligt in de aangeleverde data waarop is getraind. Als er vooroordelen (bias) in de data zitten, zal een AI-algoritme dit weerspiegelen. Als voorbeeld zou een AI-recruitment-algoritme bevooroordeeld zijn als de leerdata meer mannen in de top van bedrijven bevat. Het zou daaruit kunnen afleiden dat het beter mannen dan vrouwen kan aannemen omdat die een grotere kans hebben om door te stromen naar top. Dit soort complexiteiten maken dat AI-algoritmen vragen om extra oplettendheid en ethisch discussies.

Voor alle toepassingen van AI binnen JenV geldt, dat ze met zorg ontwikkeld en geïmplementeerd moeten worden, gezien het hoge politieke en maatschappelijke belang. In de AI-strategie staan daartoe dan ook belangrijke AI-design-principes gepresenteerd.

Onzorgvuldige toepassing van AI kan serieuze risico's opleveren. Wanneer algoritmen of artificiële intelligentie in een verkeerde context, op verkeerde wijze of met het verkeerde doel worden ingezet kan de impact groot zijn. Publieke waarden en fundamentele rechten zoals privacy, non-discriminatie, autonomie en menselijke waardigheid kunnen onder druk komen te staan waardoor burgers in de knel kunnen komen. Normering en toezicht kunnen eraan bijdragen de risico's van algoritmen te beperken. Ook zijn er risico's voor de nationale veiligheid. Criminelen of statelijke actoren kunnen AI inzetten omgeavan-

ceerde cyberaanvallen uit te voeren, of via sociale media manipuleren met bijvoorbeeld synthetische media als deepfakes. Daarom moet er ook aandacht zijn voor de manier waarop JenV die zorgvuldige, mensgerichte toepassing van AI borgt en monitort, om het risico van onzorgvuldige toepassingen van AI binnen JenV-organisaties, of in de maatschappij te voorkomen.

In de AI Strategie van JenV is opgenomen:

Betere benutting potentie AI, verantwoorde toepassingen AI inbedden, kennisniveau AI omhoog en beter voorbereid op AI (incidenten) door o.a.

- Stimuleren experimenten en hergebruik ontwikkelde diensten
- Bijdragen aan beleidsontwikkeling en EU-onderhandelingen
- Bijdragen aan strategische visie op regulering
- Bijdragen aan maatschappelijk debat
- Bevorderen van een open en kritische cultuur
- Inzetten op standaarden en richtlijnen
- Faciliteren kennisdeling en stimuleren van opleiding



3.3 Data science

Het cluster Data science omvat een aantal voor JenV relevante technologieën waarmee data verzameld, beheerd en/of bewerkt wordt. Doordat grote hoeveelheden data beschikbaar komen en met nieuwe technologieën beter geanalyseerd kunnen worden, wordt data ook wel ‘het nieuwe goud’ genoemd. Het cluster Data science ligt dicht tegen AI aan. Het is in de TechAgenda als apart cluster opgenomen, omdat databeheer en adequate dataverzameling randvoorwaardelijk zijn voor een datagedreven organisatie en voor het verantwoord toepassen van AI.

Belangrijk in dit cluster is ook data-infrastructuur. Dit omvat de manier waarop datastromen door een organisatie lopen: wat er ingeregeld is om grote hoeveelheden data op een goede manier te verwerken, data op te slaan, data beschikbaar te maken en continu zicht te hebben op de kwaliteit en samenhang van data.

Met *big data* en *data analytics* worden technieken aangeduid voor het analyseren van data ten behoeve van ‘datagedreven werken’. De data die in dit licht worden geanalyseerd komen uit bronsystemen (datamining) en zijn afkomstig van een toenemend aantal sensoren in het veld (Internet of Things). *Social media analytics* is een specifieke vorm van data-analyse gericht op de grote hoeveelheden data die met het gebruik van sociale media gegenereerd worden.

Imaging technologieën (beeldsensoren) is de verzamelnaam voor sensoren die beeld opnemen. Denk daarbij met name aan sensoren voor foto en video en infrarood. De sensoren worden steeds kleiner, krijgen steeds hogere resoluties, vinden hun toepassing in bodycams, als *wide area motion imagery* toepassing om bijvoorbeeld hele steden te monitoren, en als bewakingscamera’s. Zij zijn specifiek opgenomen in dit cluster als data-verzamelende technologie, voorafgaand aan beeldherkenning.

Robotic Process Automation tenslotte staat voor een softwareoplossing die repeterende, gestandaardiseerde en op regels gebaseerde handelingen automatiseert. Dit kan gecombineerd worden met AI, maar ook zonder AI biedt deze technologie mogelijkheden om arbeidsintensieve processen te vereenvoudigen en te versnellen.

Relevantie voor JenV

Data science is allereerst relevant in de context van de eigen kernprocessen. In de Departementale CDO Agenda¹⁴ staat verwoord dat datagedreven werken JenV in staat stelt om gericht te reageren, effectmetingen te kunnen uitvoeren, beleid te verbeteren, kernprocessen meer informatie gestuurd te maken, kruisverbanden te kunnen identificeren en verschillende disciplines van organisaties met elkaar te laten samenwerken. Allemaal vanuit een gezamenlijk doel; de samenleving rechtvaardig en veilig te houden en data beter te benutten voor de maatschappij (open overheid). Kwalitatief goede data is essentieel voor de mensgerichte, controleerbare inzet van AI.

De relevantie voor JenV bevat ook inherent de kansen voor beleid en uitvoering in algemene zin. De hele maatschappij wordt steeds meer datagedreven. Dat biedt kansen om gericht beleidskeuzes te maken, maar daarmee heeft JenV ook een rol bij het beschermen tegen inbreuk, veilige opslag en privacy.

¹⁴ De CDO agenda voor JenV is in Q1 2022 vastgesteld en komt binnenkort beschikbaar. Meer informatie via r.d.damhof@minjenv.nl



3.3 Data science (vervolg)

Kansen en risico's voor beleid en uitvoering

Naast de algemene risico's die samenhangen met het werken met data (data-infrastructuur, -opslag, -veiligheid en privacy) is een aantal meer specifieke kansen en risico's te benoemen.

Sociale media spelen een grote rol in het maatschappelijk leven, bijvoorbeeld voor onderling contact, entertainment en voor het zelf-organiserend vermogen van mensen. Uit de analyse van data afkomstig van sociale media kan men opmaken wat er speelt (facts & feelings), welke content veel aandacht krijgt van welke groepen en hoe (nep)nieuws verspreid wordt. Dit is gevoelige informatie, ook omdat het vaak om veel data gaat. Schaal is essentieel voor sociale media. Succesvolle sociale media zijn in de regel groot en groeiend. Dat maakt ze tot belangrijke en machtige sociale infrastructuren. Die infrastructuren zijn in handen van internationaal opererende commerciële BigTech bedrijven, waardoor de overheid er relatief weinig sturing op heeft en maatschappelijke waarden als privacy niet vanzelfsprekend hoog op de agenda staan. Dat vraagt een bijzondere aandacht van JenV als het gaat om veiligheid en rechtsbescherming.

Beeldsensoren verzamelen enorme hoeveelheden data. De vele camera's en beeldsensoren leveren daarbij ook risico's voor privacy. Gecombineerd met AI bieden ze een belangrijke bron voor real-time intelligence. Beeld van personen bevat inherent persoonskenmerken. Veilige opslag en verwerking van deze gegevens is daarmee van groot belang. Zeker in combinatie met de soms zwakke beveiliging van netwerken (Internet of Things) is dit een risico.

De softwarematige 'robots' onder de noemer 'Robotic Process Automation' (RPA) maken gebruik van bestaande applicaties bij het uitvoeren van gestandaardiseerde (administratieve) handelingen, net zoals een medewerker dat ook doet. Omdat de software op hoge snelheid kan werken, en 24/7 taken kan uitvoeren, worden grote efficiëntieslagen bereikt, en worden fouten verminderd. De technologie is volwassen en de expertise om de technologie in te zetten is voorhanden. Met name bij de Dienst Justitiële Inrichtingen (DJI) is veel ervaring opgedaan met deze technologie. Doorontwikkeling van RPA richt is op het combineren met artificiële intelligentie, waarbij de handelingen niet 'voorgeschreven' zijn, maar zelflerend geïnitieerd worden aan de hand van algoritmes. Dat betekent dat dezelfde risico's ten aanzien van transparantie en controleerbaarheid dan ook voor RPA gaan gelden.

Omdat de software op hoge snelheid kan werken, en 24/7 taken kan uitvoeren, worden grote efficiëntieslagen bereikt, en worden fouten verminderd.



3.4 Netwerken en infrastructuur

Veel nieuwe toepassingen maken gebruik van netwerken en fysieke infrastructuur om data over te transporteren. Dit cluster vormt als het ware een noodzakelijk fundament onder onze informatiemaatschappij. In dit fundament vindt ook substantiële vernieuwing plaats, die zowel voor JenV's uitvoeringspraktijk en bedrijfsvoering, als voor de beleidsmakers relevantie heeft.

Netwerken worden steeds verder uitgebreid met het Internet of Things. Miljarden 'dingen' zullen in de komende jaren aangesloten worden op het Internet. Onder andere met behulp van de nieuwe draadloze communicatiestandaard 5G. Tegelijkertijd worden satellieten en andere nieuwe oplossingen in de hoge luchtlagen snel goedkoper, en brengen nieuwe mogelijkheden. Onder andere voor afgelegen gebieden, of voor gebieden die door calamiteiten getroffen zijn.

Cloud computing is opgenomen als een impactvolle technologie die in de markt inmiddels breed beschikbaar is, en waar JenV aan de vooravond van implementatie staat.

Relevantie voor JenV

Onze maatschappij raakt in toenemende mate afhankelijk van steeds verder verknoopte netwerken. Daarmee neemt onze kwetsbaarheid toe voor verstoringen van allerlei aard. De grote beveiligingsrisico's van het *Internet of Things* dwingen ons tot nadenken over de kadering en de inzetbaarheid van technologieën. Rijksbreed moet JenV ook privacy waarborgen, mede door beleid te maken over nieuwe infrastructuren en netwerken en deze te handhaven.

Naast veiligheidsrisico's en risico's rond privacy, zijn de ontwikkelingen op het gebied van netwerken en infrastructuur ook cruciaal voor het bereiken van meer efficiëntie en effectiviteit van beleid en uitvoering van JenV, en voor het aangaan van diverse maatschappelijke opgaven. Niet voor niets geeft het nieuwe kabinet een stevige politieke impuls op digitalisering.

Onze maatschappij raakt in toenemende mate afhankelijk van steeds verder verknoopte netwerken. Daarmee neemt onze kwetsbaarheid toe voor verstoringen van allerlei aard.



3.4 Netwerken en infrastructuur (vervolg)

Kansen en risico's voor beleid en uitvoering

Met 5G krijgen nooddiensten snellere dataverbindingen tot hun beschikking, waarmee het mogelijk wordt om op een veilige manier bijvoorbeeld live video te versturen. Maar ook drones en andere vormen van autonome voertuigen en robots maken intensief gebruik van 5G. Het internet-of-Things biedt kansen voor monitoring en bewaking van gebouwen, objecten en gebieden doordat heel veel sensoren gemakkelijk ontsloten kunnen gaan worden, en kunnen bijdragen aan *real time intelligence*.

Satellieten bieden juist op macroschaal nieuwe mogelijkheden voor dataverzameling. Staatsbosbeheer gebruikt satellieten om tot op het niveau van individuele bomen de gesteldheid van bosgebieden te monitoren. Op het gebied van Jen V kan waarneming vanuit satellieten en andere 'low earth orbit'-apparatuur bijdragen aan beleidsinformatie, crisisbeheersing en rampenbestrijding, opsporing van bijvoorbeeld drugsafvaldumping, surveillance, herkomstonderzoek ten behoeve van migratie, detectie van uitstoot van ondergrondse drugslaboratoria.

Cloudtechnologie tenslotte biedt vooral kansen voor het verhogen van de productiviteit van ambtenaren in hun dagelijkse werk. Informatie wordt beter doorzoekbaar, data beter deelbaar, en samenwerken zal met cloudtechnologie ook een impuls krijgen. Ontwikkelingen rondom private clouds, naast de reeds bekendere publieke clouddiensten brengt kansen en keuzes met zich mee. Wat *moet* in een private cloud opgeslagen worden, wat *kan* in een publieke cloud opgeslagen worden. Wat is de impact van een combinatie van publieke en private clouds in het gebruik én hoe worden alle verplichtingen (AVG, beveiliging) in zo'n cloud-infrastructuur geborgd. En daar komen vraagstukken rond spionage, opsporing, data-retentie en data-eigendom bij.

De ontwikkelingen op het gebied van netwerken en infrastructuur brengen nog andere risico's met zich mee. Onze maatschappij raakt in toenemende mate afhankelijk van steeds verder verknoopte netwerken. Daarmee neemt onze kwetsbaarheid toe voor verstoringen van allerlei aard. En met het verder uitgroeien van de netwerken via onder andere het *Internet of Things* naar onze huishoudens, bruggen, auto's en wifi-camera's, neemt het risico op gegevensverlies of uitval toe. Veel apparaten of installaties hebben connectie met het netwerk nodig om überhaupt te functioneren. Via dezelfde netwerken die we benutten voor de hierboven aangestipte kansen, zoeken hackers en criminelen ook naar nieuwe mogelijkheden. Daarmee vormen zij een bedreiging voor onze fysieke infrastructuur en vitale sectoren of datastromen¹⁵.

Voor verstoringen van onze civiele werken als sluizen en waterzuiveringsinstallaties wordt al jaren gewaarschuwd. Ook de plaats-, tijd- en navigatie-informatie van satellieten blijkt kwetsbaar, met potentieel grote gevolgen.

Ook neemt de kans toe dat criminelen eigen autonome netwerken opbouwen: draadloze netwerken en zelfs satellieten komen binnen bereik, wat opsporing bemoeilijkt.

¹⁵ NCSC Trendlijst 2021 | [ncsc.nl](https://www.ncsc.nl)



3.5 Digitale werkelijkheid

Belangrijkste technologieën in het cluster Digitale werkelijkheid zijn de zogenaamde immersieve technologieën: Virtual Reality (VR) en Augmented reality (AR). Deze twee technologieën ontwikkelen zich snel op goed draagbare apparatuur zoals brillen, waarmee allerlei virtuele werelden kunnen worden beleefd. Dit kan compleet immersief (virtual reality) of als ‘laag’ over de fysieke wereld heen (augmented). Andere draagbare (meet)apparatuur onder de noemer ‘wearables’ bemeten onze stressniveaus, bewegingen en posities, en geven toegang tot informatiebronnen via bijvoorbeeld een Google Assistent in een smartwatch. Dit zorgt ervoor dat onze fysieke omgeving steeds meer versmelt met de digitale wereld. Zeker als onze fysieke wereld ook steeds beter gevangen is in digitale modellen (digital twins) van steden, gebieden en gebouwen.

In toenemende mate leven we ons leven nú al in een digitale werkelijkheid. Tijdens de Covid-19 pandemie hebben we al een voorproefje kunnen ervaren. We vergaderen via video, en brainstormen via whiteboard-programma's.

Technologie op dit gebied ontwikkelt zich snel door. Enorm veel kapitaal wordt ingezet door marktpartijen om onze digitale werkelijkheid aantrekkelijker, completer en gemakkelijker te maken. Men gebruikt hiervoor vaak de term ‘Metaverse’. We gaan het internet en de applicaties voor werken, sociaal interacteren en vermaak niet meer bezoeken via browsers en websites: we gaan er in toenemende mate in leven.

Relevantie voor JenV

De drie technologieën in het cluster zijn nauw verbonden met een aantal technologieën uit het AI-cluster. Immersieve technologieën, synthetische media (deep fakes), sociale media en ontwikkelingen rond de digitale identiteit (SSI) versterken elkaar.

In de nieuwe digitale werkelijkheid moet nog duidelijk worden hoe mensen daar veilig, inclusief en vrij kunnen bewegen. Of onze privacy en onze data daar veilig zijn. En wie daar gaat handhaven. De platformen zijn vaak in private handen.

Juist omdat de digitale werkelijkheid nog zo in ontwikkeling zijn, is het van belang om er als overheid mede invloed op uit te oefenen. Zodat het een digitale werkelijkheid wordt, op de Europese waarden gestoeld, zoals ook de Europese Commissie verwoordt in haar voorgestelde declaratie over digitale rechten en principes.¹⁶

Het cluster is ook relevant omdat JenV-organisaties zoals bijvoorbeeld de Politieacademie zelf trainingen en opleidingen maken, die gebruik maken van immersieve technologie.

Kansen en risico's voor beleid en uitvoering

De kracht van VR is dat je als mens ondergedompeld wordt (immersie) in een andere wereld of situatie. Het biedt kansen op het gebied van training en opleiding voor operationele diensten als brandweer en politie, maar ook bijvoorbeeld voor het begeleiden van gedetineerden op terugkeer in de maatschappij, zoals DJI laat zien. AR kan toegevoegde waarde bieden bij het (op afstand ondersteund) onderzoeken van een plaats delict. *Wearables* zijn interessant om gezondheid en stresslevels van medewerkers in de operatie te monitoren. Ook bieden ze toegang tot informatiebronnen via bijvoorbeeld digitale assistenten die in de wearables verwerkt zijn, en met spraaktechnologie zijn te bedienen.

Met de technologie onder de noemer van *Digital Twins* kan een stad, gebied of object gesimuleerd worden. Bij Digital Twin wordt niet alleen statische informatie afgebeeld, maar kunnen ook effecten, prestaties en ontwikkelingen worden voorspeld of gesimuleerd. Digital Twin vormt een gemeenschappelijke informatiebasis, waar veel overheidsdiensten hun voordeel mee kunnen doen (datadeling open overheid). Uitdaging is dat het gaat om het voorspellen van effecten. De uitkomsten worden nog niet altijd erkend voor besluit- en beleidsvorming.

¹⁶ Declaration on European Digital Rights and Principles | Shaping Europe's digital future | europa.eu



3.5 Digitale werkelijkheid (vervolg)

Risico's

Risico's van de digitale werkelijkheid liggen in het verlengde van onwenselijke aspecten van sociale media en internet op dit moment: schadelijke en illegale gedragingen in de virtuele wereld in de vorm van bedreiging, belediging en (identiteits-)diefstal, maar ook verslaving, virtuele aanranding en normvervaging liggen op de loer. Het recht lijkt redelijk goed toegerust om negatieve effecten van immersieve technologieën te adresseren op dit moment. Maar met het oog op preventie liggen er vraagstukken op het gebied van regulering en handhaving. Ook zijn er zorgen over de monopolisering van de digitale werkelijkheid door enkele grote technologiepartijen en is nog onduidelijk wat de consequenties zijn voor opsporing en bijvoorbeeld 'lawful interception'.

Inzet van immersieve technologieën en wearables leidt tot het verzamelen van grote hoeveelheden persoonsgebonden data. Medische gegevens, gedragingen in virtuele ruimtes of metingen van emoties zijn privacygevoelig. Dat brengt het risico van datalekken en oneigenlijk gebruik van deze data met zich mee.

De inzet van immersieve technologieën in de rechtszaal roept ook vragen op ten aanzien van beïnvloeding van geheugens van verdachten en daarmee de betrouwbaarheid.

In de nieuwe digitale werkelijkheid moet nog duidelijk worden hoe mensen veilig, inclusief en vrij kunnen bewegen en of onze privacy en data daar veilig zijn



3.6 Quantum

Quantumtechnologie is een verzamelnaam voor technologieën die gebruik maken van eigenschappen uit de quantummechanica. Toepassingen bestrijken een breed palet. Het is de verwachting dat deze technologieën zullen leiden tot doorbraken op het gebied van rekenkracht (digitalisering), cyber security, nieuwe materialen en (onderzoek rondom) nieuwe medicijnen.

Quantumcomputers bieden een veel grotere rekenkracht dan traditionele computers. Berekeningen die momenteel enkele weken in beslag nemen, kunnen in seconden worden uitgevoerd met behulp van quantumcomputing. Quantumcomputers kunnen namelijk veel meer data in parallelle processen tegelijkertijd verwerken. Ze zullen daarom ingezet worden voor specifieke taken. Voorbeelden hiervan zijn het zoeken in grote datasets, en analyse van zeer complexe combinatorische problemen.

Door de grote rekenkracht heeft de quantumtechnologie ook effect de manier waarop uitwisseling van data beveiligd moet worden. 'Gewone' encryptie-standaarden kunnen eenvoudig gekraakt worden. Daarom wordt geïnvesteerd in onderzoek naar quantum sleutels, als vorm van Post-Quantum Cryptografie.

Op basis van quantumtechnologie worden ook zeer nauwkeurige sensoren ontwikkeld. Zo bestaan er op dit moment al zeer nauwkeurige atomaire quantumklokken in laboratoria. De uitdaging is om deze kloksystemen robuuster en kleiner te maken, zodat ze bijvoorbeeld kunnen worden toegepast in satellieten. Dit wordt tussen de vijf en tien jaar verwacht.

Relevantie voor JenV

De volwassenheid van de technologie is nog laag. De verwachting is nu dat de Quantumcomputer over een termijn van circa 10 jaar voor JenV praktisch inzetbaar wordt. Dat lijkt erg ver in de toekomst te liggen. Quantum communicatie wordt echter eerder verwacht en ook op het gebied van sensoren wordt toegepast onderzoek gedaan.

Het is nog vroeg om met enige zekerheid concrete toepassingen van quantumcomputers te schetsen. Experts verwachten een zeer grote impact op de maatschappij, en ook op het JenV-domein. Vergelijk het met de opkomst van de (huidige) computer of de jaren '80 van het internet. Met de recente toekenning van 615 miljoen Euro uit het Groiefonds¹⁷ investeert het kabinet stevig in deze sleuteltechnologie. Internationaal zijn de investeringen nog veel groter. De verwachting is dat dit een versnelling op zal leveren in de ontwikkeling van bruikbare toepassingen.

Gezien de potentieel grote impact op (digitale) veiligheid en privacy is het actief volgen en aansluiten bij de ontwikkelingen op het gebied van quantumtechnologie van belang om in de komende jaren beter zicht te krijgen op risico's, kansen en impact.

De verwachting is nu dat de Quantumcomputer over een termijn van circa 10 jaar praktisch inzetbaar wordt.

¹⁷ quantumdelta.nl/pressreleasenl en Onderzoek, ontwikkeling en innovatie | nationaalgroiefonds.nl



3.6 Quantum (vervolg)

Kansen en risico's voor beleid en uitvoering

Quantumtechnologie is op het gebied van veiligheid potentieel disruptief, zowel positief als negatief. Kijkend naar de enorme mogelijkheden qua rekenkracht, liggen er voor JenV bijvoorbeeld kansen voor verbeterde beleidsanalyses en simulaties (voorspellingen) om misdaad te bestrijden. Maar ook criminelen en terroristen kunnen quantum-computing gebruiken voor analyses van en aanvallen op netwerken, of voor het ontwikkelen van nieuwe (chemische) wapens of drugs.

De economische veiligheid is een punt van aandacht bij quantumtechnologie: Willen EU-landen afhankelijk zijn van de quantumcapaciteit van andere landen, of zou er autonome, Europese quantumcapaciteit moeten worden ontwikkeld.

Op termijn zullen op basis van quantumtechnologie ook quantumnetwerken worden gerealiseerd, die het inherent onmogelijk maken om af te luisteren (*quantum-communicatie*). Dit is zowel een kans voor veilige overheidscommunicatie, als een bedreiging als criminelen hier gebruik van gaan maken.

Voor JenV is de ontwikkeling van zwaartekrachtsensoren onder andere relevant, waarmee detectie van ondergrondse ruimtes mogelijk wordt (denk aan opsporen drugslabs of tunnels bij gevangenissen). Ook GPS-onafhankelijke navigatie is een mogelijke ontwikkeling.



3.7 Life science technologies

Life science technologie is gebaseerd op of het gebruik van levende materialen of organen. De stand van de verschillende technieken binnen dit cluster verschilt. Voor JenV zijn vooral DNA-analyse, Genetic Engineering en Biochips (en biosensoren) van belang.

De menselijke genen zijn samengesteld uit DNA. Nieuwe DNA-*analyse*-technieken stellen ons in staat steeds sneller en goedkoper een DNA-profiel te maken. Elk mens heeft een uniek DNA-profiel. Een DNA-test kan hierdoor nu altijd herleid worden naar een individu.

Genetische manipulatie of (*precise*) *genetic engineering* is het toevoegen, verwijderen, vervangen of wijzigen van DNA in de genen van organismen. Door middel van gene editing technologie, zoals CRISPR/Cas, kunnen genen bewerkt worden en aan- of uitgezet worden in planten, dieren en mensen ('knippen en plakken van genetisch materiaal'). Deze technieken komen op korte termijn veel breder beschikbaar dan nu het geval is.

Biochips zijn in feite miniatuurlaboratoria (ook wel 'lab on a chip') die biochemie combineren met elektrische- of computertechniek, en zo veel biochemische reacties gelijktijdig kunnen uitvoeren. Hierdoor zijn grote hoeveelheden biologische stoffen te analyseren, om bijvoorbeeld ziekten te diagnosticeren of gevaarlijke biochemische stoffen te identificeren.

Biosensoren zijn apparaten die biologische of biochemische processen meten en omzetten in een elektrisch signaal. Ze kunnen voor veel doeleinden worden gebruikt, zoals nano-sensoren die ingebed zijn in slimme kleding voor de detectie van CBRN-stoffen, of een glucose-sensor voor diabetici. Fysiologische bewakingstechnologieën voor de mens zijn al commercieel verkrijgbaar en op de middellange termijn zullen meer geavanceerde sensoren beschikbaar zijn.

Relevantie voor JenV

Met DNA-analyse kregen politie en justitie een belangrijk hulpmiddel in handen bij de opsporing van verdachten. Maar het is vooral de opkomst van bedrijven die DNA-tests aanbieden aan particulieren (DirectTesttoConsumer, DTC), die voor een enorme groei van DNA-analyse heeft gezorgd. Inmiddels hebben tientallen miljoenen mensen hun DNA laten testen door bedrijven zoals 23andMe, AncestryDNA en FamilyTreeDNA. Het doorverkopen van DNA-gegevens is voor deze bedrijven een belangrijke inkomstenbron. DNA dat is ingestuurd voor een persoonlijke analyse, wordt soms ook voor andere doeleinden gebruikt. Steeds meer DNA-gegevens raken op deze wijze verspreid, zonder dat er zicht is op wat er precies met dit DNA gebeurt. Terwijl voor het beheer en gebruik van DNA-gegevens door politie en justitie strikte regels gelden, is dit vooralsnog niet het geval voor gegevens uit commerciële DNA-tests.

Genetic engineering biedt voor medische toepassingen grote potentie, bijvoorbeeld bij het genezen van erfelijke ziektes of kanker. Tegelijkertijd roept dat direct ethische vraagstukken op over hoever mensen daarin mogen gaan. 'Kiembaanmodificatie' waarbij het DNA van mensen blijvend veranderd kan worden, bijvoorbeeld om erfelijke aandoeningen te voorkomen, is verboden in Nederland.

Steeds meer DNA-gegevens raken verspreid, zonder dat er zicht is op wat er precies met deze data gebeurt.



3.7 Life science technologies (vervolg)

Kansen en risico voor beleid en uitvoering

Naast de evidente kansen van (snellere of mobiele) DNA-analyse, zijn er vraagstukken rondom het strafrechtelijk gebruik van DNA-data die door commerciële bedrijven zijn vergaard (investigative genetic genealogy of IGG). Hoewel hiermee successen zijn behaald in vastgelopen moordzaken is het duidelijk dat lang niet iedereen die materiaal opstuurt naar een DTC-bedrijf een dergelijke toepassing voorziet. Omdat DNA per definitie gedeeltelijk identiek is aan het DNA van verwanten, raakt dit niet alleen degenen die ervoor kiezen het DNA in te sturen, maar ook hun familieleden. Verwanten worden echter niet systematisch geïnformeerd en aan verwanten wordt in het algemeen geen toestemming gevraagd.

Burgers hebben nu geen universele en onvervreembare zeggenschap over hun DNA, terwijl ze de consequenties van de verspreiding van DNA slechts beperkt kunnen overzien. Bij het verzamelen, analyseren en vertalen van DNA-gegevens zou bescherming van privacy wettelijk geregeld moeten zijn en dient genetische discriminatie te worden voorkomen. Ook moeten de verantwoordelijkheden voor degenen die DNA-gegevens toepassen, duidelijk worden omschreven.

Risico's voor genetic engineering zijn, naast de ethische vraagstukken, ook dat lange termijneffecten van genetische aanpassingen nog niet genoeg getest zijn. DNA is complex, dus aanpassingen kunnen zeer veel effecten hebben op zeer veel gebieden waarbij het nu nog bijna onmogelijk is om gevolgen van vergaande manipulatie te overzien. Daar komt bij dat veel onderzoek nu uitgevoerd wordt door private bedrijven met een duidelijke winstoogmerk. Genetische data wordt mogelijk verzameld, met privacy aspecten tot gevolg.

Kansen voor Biochips en Biosensoren liggen voorsnog vooral op het gebied van Human Enhancement Technologies (HET). Hierbij gaat het om biomedische interventies met als doel menselijke functies te verbeteren. Het kan gaan om het versterken van fysieke, cognitieve en sociale functies. Toepassingen worden voorzien voor first-responders, en voor biosensoren mogelijk ook in het kader van bijvoorbeeld detentie onder voorwaarden (mogelijke ontwikkeling drugs- of alcoholensoren).



3.8 Engineering technologies

In dit cluster zijn twee brede technologieën opgenomen, die in elkaars verlengde liggen: robots en autonomous vehicles & systems. Beide maken gebruik van een scala aan eerder genoemde technologieën zoals AI, sensortechnologie en bijvoorbeeld 5G.

Robots zijn programmeerbare machines die eenvoudige en inmiddels ook complexe taken kunnen uitvoeren. Er zijn robot-armen, robotplatforms, robots als verlengstuk van het menselijk lichaam (onder andere exo-skeletten) robots in de vorm van een mens (antropomorfe robots), nano- en micro-robots.

In het verlengde van robots liggen de autonome voertuigen. Dit zijn voertuigen die zich zelfstandig voortbewegen, dus zonder menselijke chauffeur, piloot of schipper. Er is onderscheid in verschillende categorieën autonome voertuigen, namelijk: wegvoertuigen (auto's, trucks en bussen), vliegende voertuigen (drones, drone-taxi's) en varende voertuigen (boten en voertuigen voor onder water, zoals onderzeeërs en onderwater drones).

Relevantie voor JenV

Robots en autonome systemen zoals drones doen gestaag hun intrede in onze maatschappij. Ze bieden kansen in de uitvoering, zoals bijvoorbeeld de inzet van een blusrobot, die nooit vermoeid raakt of inzet van vliegende drones door de politie voor crowd-control en observatie. Kwaadwillend gebruik van dezelfde systemen is de andere kant van de medaille.

De ethische, juridische en maatschappelijke vraagstukken rond robots en autonome systemen vragen om beleidsmatige betrokkenheid van JenV in de komende jaren. Deels overlappen die vraagstukken met de vraagstukken zoals aangestipt bij AI, maar het betreft ook bijvoorbeeld vraagstukken rond aansprakelijkheid in het fysieke domein.

Kansen en risico's voor beleid en uitvoering

Robots nemen de zogenaamde 'dull, dirty of dangerous' taken over van mensen. Naast beveiligings- en brandbestrijdingstaken vormt de inzet van robotica in de toepassing 'exo-skeletten' een aparte categorie, waarmee onder andere het Ministerie van Defensie experimenteert. In deze toepassing werken mens en robot werken nauw met elkaar samen (man-machine-teaming): de robotpakken van defensie worden gedragen door soldaten om bijvoorbeeld zware munitiekisten te tillen. Dit soort toepassingen zijn ook voor de zorg en voor first-responders interessant.

Een heel andere toepassing is de sociale robot, waarmee zowel politie als DJI experimenten mee heeft uitgevoerd. Dit betreft robots die vooral zijn ontwikkeld om te interacteren met mensen. In deze toepassing kunnen robots mensen vervangen of ondersteunen als aanspreekpunt bij balies of als 'maatje' voor geïnterneerden. Het biedt een perspectief op het vervullen van specifieke taken in een lastige arbeidsmarkt.

Op een mens gelijkende (antropomorfe) robots leiden ook tot andere vraagstukken. Het Rathenau-instituut werpt bijvoorbeeld de vraag op of seks-robots al dan niet moeten worden toegestaan, en of deze bijvoorbeeld uitsluitend een volwassen uiterlijk zouden mogen hebben.

Van de verschillende modaliteiten van *autonome voertuigen en systemen* zijn met name de zelfrijdende auto's (*voertuigen*) en vliegtuigen (drones) ver ontwikkeld. Deze toepassingen laten zien dat er allerlei maatschappelijke kansen liggen op het gebied van mobiliteit, verkeersveiligheid en emissiereductie. JenV's uitvoeringsorganisaties zetten inmiddels met name drones breed in voor observatie en inspectietaken. De kansen voor de overige modaliteiten zullen zich in de komende jaren ontfouwen. Het is zaak om met beleid en wetgeving bij te blijven bij lopende ontwikkelingen in de maatschappij.



3.8 Engineering technologies (vervolg)

Feit is dat al deze automatische systemen heel veel data verzamelen via sensoren. Die informatie kan – mits verantwoord benut – van grote toegevoegde waarde zijn. Denk bijvoorbeeld aan de data van (semi-)zelfstandig rijdende auto's, die waardevol is voor meldkamers.

Risico's van autonome systemen liggen met name op veiligheidsgebied; luchtvaartveiligheid en gebruik door kwaadwillenden. Met name vliegende drones zijn gemakkelijk verkrijgbaar. Het voorkomen van aanslagen op personen of vitale infrastructuur, of het tegengaan van smokkel met behulp van drones is een actuele uitdaging voor JenV.

Net als bij robots zijn er bij autonome voertuigen en systemen diverse kwesties op het terrein van recht, privacy, cybersecurity en ethiek (denk bijvoorbeeld aan bewapende drones).

Het voorkomen van aanslagen op personen of vitale infrastructuur, of het tegengaan van smokkel met behulp van drones is een actuele uitdaging voor JenV.



4

Handelingsperspectief voor het technologieportfolio

De TechAgenda helpt bij het prioriteren en geeft richting aan het Technologie Adaptatie Proces¹⁸. In hoofdstuk 3 van deze TechAgenda zijn de geprioriteerde technologieën toegelicht. Met het doel in gedachten om tijdig te kunnen *acteren* op deze technologieën wordt in dit hoofdstuk perspectief geboden op manieren om te handelen op de verschillende technologische ontwikkelingen.

¹⁸ Het proces van technologieadaptie (TAP) richt zich op het leren over de impact van specifieke technologieën. Zie de Whitepaper 'Focus op technologie' op www.innoveermeemetjenv.nl/technologie

4.1 Acteren in verschillende vormen en intensiteiten

Het handelingsperspectief voor JenV kan er per technologie verschillend uitzien. Het is afhankelijk van de mate van volwassenheid van de technologie, de specifieke impact die verwacht wordt, en hetgeen er reeds gebeurt binnen JenV rondom een specifieke technologie.

Op veel van de gesignaleerde technologieën lopen al initiatieven binnen JenV. Voor een aantal technologieën zijn aanwijsbare teams opgesteld (zoals bij AI) of is een onderzoeksprogramma gedefinieerd bij TNO (zoals rond robotica). Voor andere technologieën is minder goed aan te geven dat we als JenV al aan het acteren zijn, of ons voorbereiden.

Aard en volwassenheid van een technologie

De aard en volwassenheid van een technologie (ook wel Technology Readiness Level of TRL¹⁹) bepaalt wat de meest effectieve actie is. Bij een jonge technologie is dat bijvoorbeeld eerdere investeren in onderzoek en ontwikkeling, al dan niet samen met kennisinstellingen en bedrijven (denk aan topsectorenbeleid). Bij meer volwassen technologieën kan ook experimenteren aan de orde zijn, maar is ook het stellen van beleidsmatige kaders (normatief optreden) relevant. Daarbij is ook de aard van de technologie van belang: in de lijst van geselecteerde technologieën bevinden zich zowel concrete toepassingen, als bouwstenen, concepten en meer fundamentele ontwikkelingen.

Wat er al gebeurt rondom een technologie

Het 'Organisational Readiness Level' (ORL)²⁰ geeft een indicatie wat er al gebeurt rondom een technologie en in hoeverre JenV zelf al actief is. Een eerste analyse van het ORL, geordend in drie delen, is uitgevoerd en opgenomen in bijlage 4. Deze drie delen: wat is er aan netwerk/ecosysteem; hoe staat het met kennis en onderzoek en is er een gestructureerde aanpak, zijn omschreven in tabel 4.1.

Tabel 4.1: Organisational readiness

Netwerk/ecosysteem	Kennis/Wetenschap / onderzoek	Aanpak JenV
Is er een netwerk (operationeel, beleid, interdepartementaal, en/ of binnen JenV)?	Is/wordt er onderzoek gedaan met/in opdracht van JenV?	Is er een trekker binnen JenV / is het duidelijk belegd?
Is er een gezamenlijke interdepartementale aanpak?	Is er verbinding met de wetenschap?	Is er een actieplan/ visie / strategie (lees: gecoördineerde aanpak)?
Vinden er experimenten/ innovatieprojecten plaats? Binnen de overheid, wetenschap, private partijen?	Zijn er onderzoeksrapporten beschikbaar over kansen, risico's en maatschappelijke consequenties?	Is er voldoende personele capaciteit op het onderwerp?
Is er aandacht voor de technologie in de EU of daarbuiten?		Is er kennis binnen JenV over de technologie?

19 TRL, of technology readiness level geeft een beeld van de volwassenheid van een technologie. TRL 1 bijvoorbeeld staat voor een technologie in de kinderschoenen, die alleen nog 'op papier' in de academische wereld bestaat. TRL 6 staat voor een technologie die al in een relevante context is uitgetoet. TRL 9 staat voor een geïmplementeerde technologie

20 ORL, of Organisational Readiness Level wordt gebruikt om een beeld te geven in hoeverre de succesfactoren in en om een organisatie aanwezig zijn om een verandering of een innovatie te implementeren.

Is de impact nog niet helder, dan is een goede start om te participeren in een (bestaand) netwerk rondom de technologie.

Bovenstaande leidt tot de volgende opbouw van mogelijke handelingsperspectieven:

1. Participatie in een bestaand technologienetwerk en/of opstarten van een netwerk/team binnen JenV
2. Ontwikkelen kennis (intern en/of extern)
3. Ontwikkelen beleid en/of wet- en regelgeving
4. Experimenteren en innoveren

Niet elke variant van acteren is altijd noodzakelijk. Soms is er al veel kennis en onderzoek uitgevoerd, of is ontwikkelen van wet- en regelgeving niet aan de orde. Er zit wel samenhang in. Om goed op de hoogte te raken van (de impact van) een technologie is aansluiten bij een (interdepartementaal) netwerk aan te bevelen. Afhankelijk van de impact is het daarna, of daar naast, ook van belang kennisuitwisseling binnen JenV te organiseren. De volgende stappen kunnen verschillen per specifieke technologie: is kennisontwikkeling noodzakelijk; moet er beleid ontwikkeld worden, en/of is het beter te starten met experimenteren.

Participatie in bestaand technologienetwerk en/of opstarten JenV-team

Voor een aantal technologieën is deelname aan een bestaand technologienetwerk voldoende. Denk aan de werkgroep technologieverkenningen van de Rijks Innovatie Community (WGTv), DigiCampus of een PPS-coalitie. In zo'n netwerk kan inzicht in de materie worden vergroot, en kunnen betere inschattingen gemaakt worden ten aanzien van het vervolg. Dit vergt beperkte capaciteit en middelen.

Vaak is JenV's organisational readiness ook gebaat bij netwerkgericht leren binnen JenV zelf, ook als er geen interdepartementale tech-community bestaat. In dit geval kan het relevant zijn zelf een (virtueel) team of netwerk te vormen van (in eerste instantie) enkele JenV-ambtenaren met het meest directe belang. Dit kan binnen JenV uitgroeien naar een tijdelijk beleidsteam zoals rond AI en/of naar een (inter-)departementale werkgroep, die bedrijfsleven en kennisinstellingen nauw betreft.

Voorbeeld: Quantumtechnologie

Rondom quantumtechnologie zijn diverse netwerken actief. Onder andere de rijksbrede Quantum Innovation Hub Rijksoverheid, en Quantum Delta zijn interessante omgevingen om aangesloten te blijven op de ontwikkelingen, en een beter zicht te krijgen op kansen, risico's en impact voor JenV.

Ontwikkelen kennis

Voor een goede positiebepaling van JenV ten aanzien van een technologische ontwikkeling, komen vroeg of laat lastige vragen naar voren. Sommige kennisvragen hebben een beleidsondersteunend karakter, zoals de vraag rond Immersieve technologie naar het te verwachten (schadelijke) gedrag van mensen in virtuele ruimtes, naar aanleiding van een motie in de Tweede Kamer²¹. Andere kennisvragen zijn meer van toegepaste aard, zoals de vraag welke waardevolle ervaringen er in het buitenland zijn met robots ten behoeve van bewakingstaken. Een goede vraagstelling is essentieel om passende kennisvragen in te brengen bij denktanks of kennisinstellingen.

Voorbeeld: Immersieve technologie

Om in te kunnen schatten of bestaande juridische kaders en wetgeving in de nabije toekomst moeten worden aangepast als gevolg van de snelle ontwikkelingen van immersieve technologie en virtuele werelden (o.a. Metaverse), is aanvullend onderzoek nodig naar met name het te verwachten (schadelijke) gedrag van mensen in virtuele ruimtes, en naar de wijze waarop data wordt opgeslagen op de nieuwe platforms.

²¹ Kamerstukken II 2019/20, 35 300 VI, nr. 73

Ontwikkelen beleid en/of wet- en regelgeving

Voor een aantal technologieën geldt dat het relevant kan zijn om een toets uit te voeren op het huidige regime van wet- en regelgeving. Indien geconstateerd wordt dat aanvullend beleid nodig is, kan advies uit de toets ter hand genomen worden. Hier ligt een kans om van reactief beleid naar pro-actief beleid te komen. Eerdere kennisontwikkeling en/of deelname aan een bestaand netwerk gaan in de tijd vooraf. Dit kan significant bijdragen aan versnelling en verbetering van nieuw beleid en/of wet- en regelgeving.

De beleidsontwikkeling binnen JenV heeft niet alleen betrekking op toepassing van technologie binnen het ministerie zelf. Juist daar waar technologie in de maatschappij bijdraagt aan de veiligheid van burgers, is beleidsontwikkeling op technologie relevant.

Voorbeeld: Gezichtsherkenning

Gezichtsherkenning is zowel relevant vanuit het perspectief van de kansen voor JenV-organisaties, zoals opsporingsdiensten, als voor de toepassing van de technologie in het maatschappelijk verkeer. Het Nederlandse beleid voor de toepassing van gezichtsherkenning (verboden tenzij), is tot stand gekomen onder invloed van Europese beleidskaders van de European Data Protection Board.

Experimenteren en innoveren

Voor een aantal technologische ontwikkelingen geldt dat een hogere mate van betrokkenheid van JenV wenselijk is via experimenteren en leren. Het betreft ontwikkelingen die het hart van JenV-raken (rechtstaat, rechtvaardigheid, privacy, veiligheid), waar veel impact van wordt verwacht (in positieve of negatieve zin), en die niet kunnen blijven liggen (hoge urgentie). In veel gevallen zijn uitvoeringsorganisaties er al mee aan de slag, en is het zaak om experimenten op deze onderwerpen te stimuleren en te verbinden, en beleid aan te sluiten.

Voorbeeld: Privacy Enhancing Technologies (PETs)

Privacy Enhancing Technologies (PETs) maken het mogelijk om met data de informatiekraft van het ministerie te versterken én de privacy van burgers te beschermen. Er wordt nu ervaring opgedaan met pilots rond JenV-casuïstiek, wat kan leiden tot gemeenschappelijke dienstverlening.

4.2 Opschalen: van ‘ontwikkelen’ naar ‘realiseren’

Op enig moment is een technologie geen nieuwe ontwikkeling meer, maar klaar om onderdeel te worden van de reguliere business van JenV. In veel gevallen is de technologie dan ook al veel breder in de maatschappij in gebruik. Dat betekent niet dat deze technologie geen aandacht meer nodig heeft vanuit beleid of vanuit bedrijfsvoering. Vaak is in een dergelijke situatie juist nog veel blijvende aandacht nodig om daadwerkelijk tot impact te komen.

Voorbeeld: Big data & data analytics

Op het gebied van datagedreven werken is veel te doen. Er is een datalab binnen JenV, dat kennis en vakmanschap ontwikkelt van data-analisten, en bruikbare data-analyses oplevert voor JenV-organisaties. De technologie is beschikbaar; de toepassing en gebruik is succesvol gebleken, maar kan nog (veel) verder groeien. Dit vergt aandacht vanuit beleid om het datagebruik binnen JenV effectiever te maken, met afdoende waarborgen voor kwaliteit en legitimiteit.

4.3 Monitoring en sturing

Met de oplevering van de TechAgenda start het proces van gebruik van de TechAgenda. Het streven is dat beleidsafdelingen, ketens en/of organisatieonderdelen door met de TechAgenda aan de slag te gaan beter begrip krijgen van impact en relevantie van de geprioriteerde technologieën voor het eigen werkveld. Zo kan een actieve houding worden ontwikkeld ten aanzien van de mogelijkheden en risico's.

De Innovation Board van JenV monitort periodiek de mate van technologie-adaptatie van JenV voor de geprioriteerde clusters technologieën. Op regelmatige basis zullen impact en urgentie opnieuw gewogen worden. Door trends en technologieën te monitoren en te beoordelen samen met de WGTV, en door nog beter gebruik te maken van beschikbare technologiescans binnen en buiten de JenV organisatie kan ook het proces van de TechAgenda nog verder verbeterd worden. Met als doel technologieën te onderzoeken, kennis te ontwikkelen, ermee te experimenteren en ze uiteindelijk te beleggen in de reguliere processen. Zo realiseren we een gecoördineerde portfoliobenadering, gemonitord vanuit de Innovation Board. In de Innovation board worden handelingsopties voorbereid, en in onderlinge afstemming taken verdeeld. Indien nodig kunnen zaken ter besluitvorming worden geagendeerd in besluitvormende gremia van JenV zoals de CIO-Raad, Brede Bestuursraad of één of meer Directoraten-Generaal.

Als 'werkagenda' zal de TechAgenda periodiek herijkt moeten worden. Daarbij wordt gedacht aan een termijn van 3 jaar (2025). Dan kan opnieuw een 'foto' gemaakt worden van de meest belangrijke technologieën voor JenV. Dit met input van vele medewerkers vanuit beleid, uitvoeringsorganisatie en externe (kennis-) organisaties.

Bijlage: Gevolgd proces

Om te komen tot deze TechAgenda heeft het projectteam van de Directie Innovatie, Kennis en Strategie een iteratief proces gevolgd. Gedurende het traject is de aanpak op basis van voortschrijdend inzicht op een aantal punten bijgesteld. In deze bijlage worden de verschillende processtappen beschreven.

1. Een basislijst voor de Rijksoverheid

In 2020 ontwikkelde de Werkgroep Technologieverkenningen (WGTV) van de Rijksinnovatiecommunity (RIC) een Technologiescan voor de Rijksoverheid. Startend vanuit een lijst van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), en de Technologiescan JenV uit 2018, is de lijst aangevuld en gevalideerd aan de hand van beschikbare onderzoeken, rapporten en gesprekken met experts. Deze Rijksbrede Technologiescan heeft uiteindelijk een lijst van 60 technologieën opgeleverd (Tabel 1), te vinden www.techfocus.nl

Op deze lijst staat een breed scala aan fundamentele technologieën; (clusters van) concrete toepassingen; bouwstenen en in een enkel geval van op technologie gebaseerde concepten of werkwijzen. Herkenbare clusters van technologieën zijn o.a. artificiële intelligentie; blockchaintechnologieën; quantumtechnologieën; autonome systemen en life sciences.

Tabel 1: TechScan Rijksoverheid (bron: Werkgroep Technologieverkenningen Rijksinnovatiecommunity)

Categorie	Technologie
Quantumtechnologie	Quantum computing
	Quantum communicatie
	Quantum sensoren en metrologie
Geavanceerde materialen	Slimme/zelf genezende/zelf-organiserende materialen
	Design en metamaterialen
	Structural materials
	Energie omzetting materialen
	Energie opslag materialen
Digitale technologieën	Blockchain incl. encryptie
	Cloud en high performance grid computing
	Big data en data analytics incl. Datavisualisatie
	Mobiele data incl. 5G
	Digital ID incl. iris scans, vingerafdrukken en self-sovereign identity
	Digital security en cybersecurity
	Privacy enhancing technologieën
	Cryptocurrencies
	Robotic Process Automation (RPA)
	Smart contracts
	Artificial Intelligence
Predictieve analyse	
Profiling	
Beslisalgoritmes en expertsystemen	
Natural language processing	
Beeldherkenning	
Synthetic media	
Communicatie	Social media en social media analytics
	Apps
	Videoconferencing en video dienstverlening
	Telepresence en avatars
	Digitaal samenwerken
	Chatbots en persoonlijke assistent
Sensor technologieën	Imaging technologieën incl. camera, infrarood, radar, WAMI
	Sniffing en particle detection
	Locatie
	Overig incl. warmte, akoestisch, draadloos (WiFi/RFID)
Fotonica	Fotonica
Nanotechnologieën	Nanotechnologieën
Chemische technologieën	Chemische technologieën
Life science technologieën	Industriële biotechnologie
	Genen bewerking en genetische engineering
	Synthetische cel technologie
	Life extension incl. nanomedicijnen
	Biochips and biosensors incl. orgaan op een chip
	Stamcel technologie
Engineering- en fabricagetechnologieën	Imaging technologieën incl. camera, infrarood, radar, WAMI
	DNA-analyse
	Robots incl. man-machine teaming
	Autonomous vehicles & systems
Mens & Technologie	3D printen
	Virtual reality, Augmented reality
	Wearables
	Exoskeletonen
Slimme omgeving	Brain imaging, brain machine interfacing
	Internet of Things
	Domotica
	Smart grids
	Smart cities
	Digital twin
Satellieten incl. Low Earth Orbit	

Deze lijst is gebruikt als uitgangspunt om toe te werken naar een prioritering voor de TechAgenda JenV. In overleg met de Stichting Toekomstbeeld der Techniek (STT) en TNO is gekozen voor een Delphi-methode met een vragenlijst (enquête). In deze enquête hebben wetenschapsjournalisten, de medewerkers van het projectteam inclusief vertegenwoordiging van TNO en STT alle 60 bovenstaande technologieën beoordeeld op 2 factoren:

- Impact: wat is de omvang van de impact van de technologie/ontwikkeling op de taakvelden van JenV (lijst van 10 taakvelden)?
- Urgentie: hoe urgent is het voor de taakvelden van JenV (lijst van 10 taakvelden) om op deze technologie in te zetten?

Door ook wetenschapsjournalisten in deze enquête mee te nemen, is naast input van specialisten ook breed georiënteerde input meegenomen. Onderkend risico daarbij was dat zij mogelijk niet alle technologieën en de relevantie voor JenV tot in de haarvaten doorgronden.

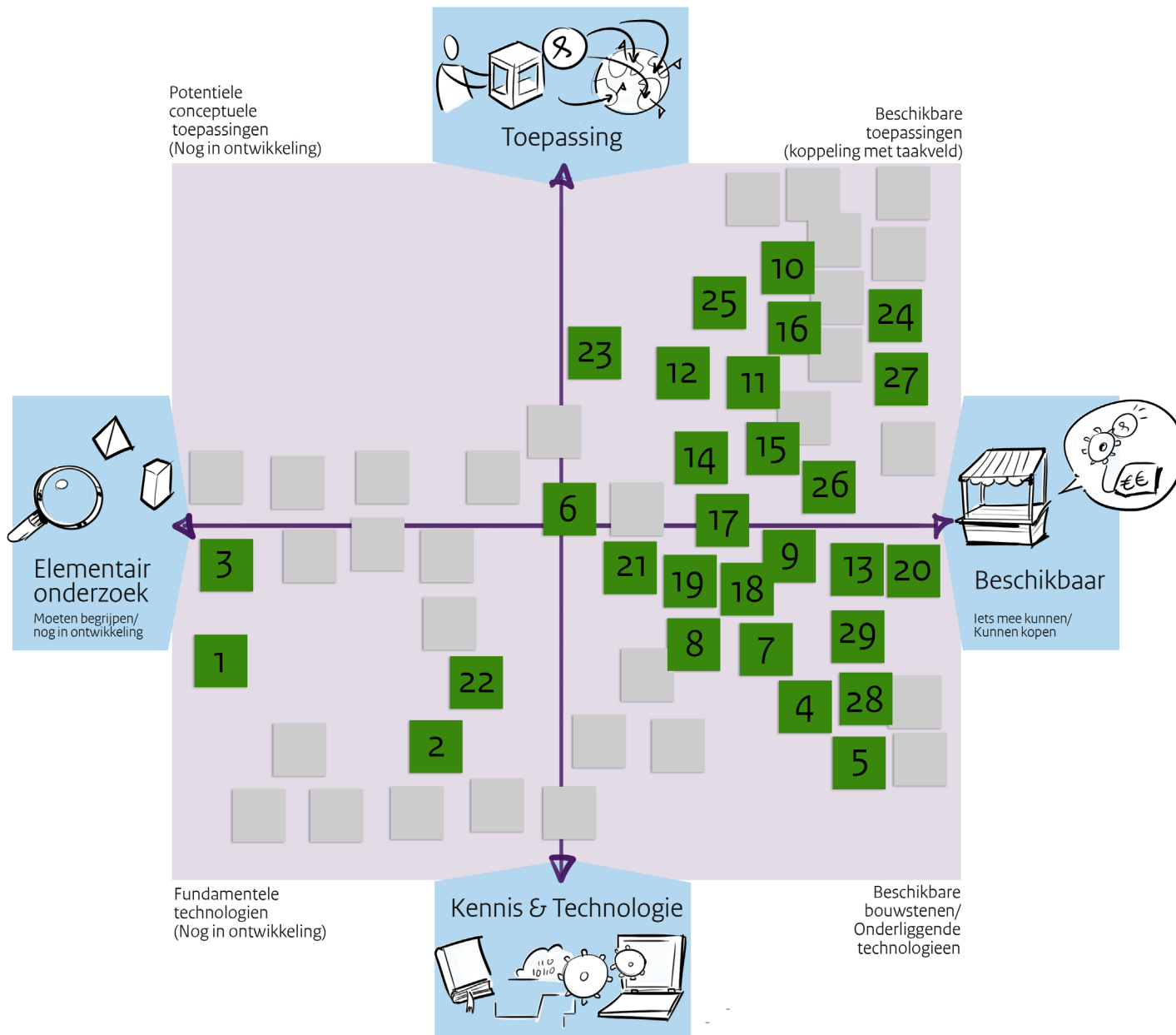
Alle uitkomsten van deze enquêtes zijn geanalyseerd en onderverdeeld in tranches. Daarbij bleek dat de basislijst van technologieën die als uitgangspunt gehanteerd is, niet eenduidig gedefinieerd is. Er kwam overlap tussen de technologieën en tegelijkertijd onduidelijkheid over de inhoud van technologieën aan het licht. Dit leidde ook tot de conclusie dat het lastig is om de technologieën met elkaar te vergelijken.

2. De long list voor JenV

Op basis van analyse van de enquêtes is de lijst van technologieën ruwweg in twee delen verdeeld. Daar waar de uitkomsten van de enquêtes en de gesprekken meer dan 'neutraal' waren heeft het team de technologie / ontwikkeling opgenomen in de *long list*.

Tabel 2: Long List Selectie JenV

Categorie	Technologie
Quantumtechnologie	1. Quantum computing
	2. Quantum communicatie
	3. Quantum sensoren en metrologie
Digitale technologieën	4. Blockchain incl. encryptie
	5. Big data en data analytics incl. Datavisualisatie
	6. Mobiele data incl. 5G
	7. Digital ID incl. iris scans, vingerafdrukken en self-sovereign identity
	8. Digital security en cybersecurity
	9. Privacy enhancing technologieën
	10. Cryptocurrencies
	11. Robotic Process Automation (RPA)
	12. Smart contracts
	Artificial Intelligence
14. Predictieve analyse	
15. Profiling	
16. Beslisalgoritmes en expertsystemen	
17. Natural language processing	
18. Beeldherkenning	
19. Synthetic media	
Communicatie	20. Social media en social media analytics
Sensor technologieën	21. Imaging technologieën incl. camera, infrarood, radar, WAMI
Life science technologieën	22. Genen bewerking en genetische engineering
	23. DNA-analyse
Engineering- en fabricagetechnologieën	24. Robots incl. man-machine teaming
	25. Autonomous vehicles & systems
Mens & Technologie	26. Virtual reality, Augmented reality
	27. Wearables
Slimme omgeving	28. Internet of Things
	29. Satellieten incl. Low Earth Orbit



Figuur 1: Overzicht technologische ontwikkelingen. Positie technologieën heeft invloed op handelingsperspectief. In deze figuur zijn de technologieën uit tabel 2 in een assenstelsel weergegeven.

De technologieën zijn in figuur 1 in vier kwadranten geplaatst, op basis van volwassenheid van de technologie (van elementair onderzoek tot algemeen beschikbaar) op de ene as en concrete toepasbaarheid op de andere as (van kennis & technologie, naar concrete toepassing).

Het mogelijk handelingsperspectief voor JenV heeft een relatie met de positie in het landschap. De technologieën in het kwadrant **rechtsboven** zijn in de meeste gevallen zo volwassen, dat er vrij gebruik van gemaakt kan worden. Door JenV, maar ook in de maatschappij. Voorbeelden zijn wearables; robots of 3D printing, maar ook een dienst als social media.

Rechtsonder bevinden zich meer de concepten, componenten en bouwstenen waardoor toepassingen in het kwadrant rechtsboven mogelijk worden. Voorbeelden zijn Blockchain, Big data en/of de Cloud computing. Ook beeldsensoren zijn een voorbeeld van een bouwsteen: de ontwikkeling van betere en kleinere sensoren leidt tot een heel scala aan toepassingen. Hierbij is het van belang dat JenV zich voorbereidt op de effecten van potentiële toepassingen die ontwikkeld worden.

Het kwadrant **linksonder** zijn veelal technologische ontwikkelingen die minder volwassen zijn en in een onderzoeksfase zitten. Dit is vooral het terrein van kennisinstellingen. Voorbeelden zijn technologieën op het gebied van genetic engineering, ontwikkeling van materialen en quantumtechnologieën. Voor JenV is kennisopbouw en het (laten) uitvoeren van verkenningen belangrijk.

In het kwadrant **linksboven** zouden concrete toepassingen een plek kunnen vinden, die al wel voorstelbaar, maar nog niet realiseerbaar zijn. Bijvoorbeeld een volledig autonoom vliegende bezorgdrone of het smart grid. Vaak zijn dit concepten of toepassingen die gebruik maken van technologieën uit de onderste helft van het overzicht en zijn ze als zodanig niet als aparte technologische ontwikkeling opgenomen in de totaal lijst.

3. Samenhang in clusters

In de daaropvolgende workshops met (i) het team en (ii) de bredere organisatie is gewerkt met de long list van technologieën.

In workshops met onder andere het AI-team, vooroverleg Innovation Board en het Architectenforum van de CIO-raad is onderzocht wat de belangrijkste technologieën van nu, morgen en overmorgen zijn voor de verschillende taakvelden van JenV, en wat daarbij de gemene delers zijn voor (bijna) alle taakvelden.

Het doel daarbij was niet om een lijst te maken waarbij de ene technologie als belangrijker wordt geduid dan een andere, maar om de organisatie een richtlijn mee te geven bij het maken van beslissingen op het gebied van inzet van capaciteit en middelen.

Op basis van de feedback uit deze workshops is gekozen om op een iets hoger abstractieniveau te clusteren: nieuwe clusters om de belangrijkste technologieën bij elkaar te houden. Door ook te kijken naar taakvelden konden ook specifieke technologieën worden opgenomen als cluster.

Deze clusters zijn hieronder op volgorde van relatieve prioriteit opgenomen. Deze relatieve prioriteit is het resultaat van de oorspronkelijke enquête, de onderliggende inschattingen van impact en urgentie en de relatie met de taakvelden.

Daarnaast is een aantal technologieën als ‘special’ te definiëren die voor een specifiek domein of taakveld relevant zijn. Deze technologieën staan in relatieve prioriteit dus niet ‘onder’ de 6 gedefinieerde clusters, maar staan er, voor het deel van de organisatie waarvoor ze relevant zijn, naast.

Tabel 3: Clusters voor JenV

Clusters TechAgenda		Technologie
 1. Digitale veiligheid	Technologieën met impact op de veiligheid van digitalisering, gegevensuitwisseling, communicatie, identificatie, dataopslag en gebruik van netwerken en infrastructuur	Digital ID en self-sovereign identity Post-Quantum Cryptografie/PQC Digital security en cybersecurity Privacy enhancing technologieën Blockchain
 2. Artificiële intelligentie	Technologieën die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken.	Synthetic media Beeldherkenning Predictieve analyse Profiling Natural language processing Beslisalgoritmes en expertsystemen
 3. Data science	Technologieën waarbij veel data verzameld en/of geanalyseerd worden. Ten opzichte van het cluster artificiële intelligentie ligt de focus bij data science minder op intelligent gedrag van de systemen.	Social media en social media analytics Big data en data analytics incl. Datavisualisatie Imaging technologieën incl. camera, infrarood, radar, WAMI Robotic Process Automation (RPA)
 4. Netwerken en Infrastructuur	Technologieën die bijdragen aan noodzakelijke verbindingen voor verdergaande digitalisering. De technologieën in dit cluster zijn daarmee randvoorwaardelijk voor veel andere ontwikkelingen	Internet of things Satellieten incl. Low Earth Orbit 5G Cloud en high performance grid computing
 5. Digitale werkelijkheid	Technologieën die bijdragen aan een digitale omgeving waarin men leeft, werkt of ontspanning zoekt, en waarin veiligheid, privacy en recht aandacht vereisen. Denk aan de Metaverse. Digitale werkelijkheid heeft directe relatie met artificiële intelligentie en sociale media	Virtual reality, Augmented reality Wearables Digital twin
 6. Quantum	Technologieën die gebruik maken van eigenschappen uit de quantummechanica. Dit cluster omvat specifiek de ontwikkeling van de sleuteltechnologie 'Quantum' (-computing, -communicatie en -sensoren)	Quantum computing en communicatie Quantum sensoren en metrologie
Specials TechAgenda		Technologie
 7. Life sciences	Technologieën die gebaseerd zijn op of gebruik maken van menselijk materialen en organen	DNA-analyse Biochips Genetic Engineering
 8. Engineering technologies	Technologieën met een fysieke verschijningsvorm. Robots, drones, autonome voertuigen en vaartuigen	Robots Autonomous vehicles & systems

In de workshops is aandacht besteed aan de impact op specifieke taakvelden van JenV. De impact van een technologie voor de verschillende taakvelden, organisatieonderdelen en uitvoeringsorganisaties kan sterk verschillen. De impact van drones in opsporing, handhaving of uitvoering van straffen ziet er anders uit dan in rechtspleging en rechtsbescherming. En het maakt ook uit of het perspectief wordt gehanteerd van kansen en risico's voor de taakuitoefening van JenV zelf, of bij gebruik in de maatschappij.

Een eerste analyse leidt tot onderstaande matrix (zie tabel 4), waarin weergegeven wordt welke technologieën over de grootste breedte van JenV impact hebben. Deze tabel vormt de start voor de verdieping met de verschillende taakvelden. De uitdaging bij de uitwerking bleek tweeledig: (i) Idealiter wordt deze analyse in viervoud gedaan: voor kansen en risico's bij gebruik in maatschappij en kansen en risico's voor JenV zelf. (ii) Afhankelijk van invalshoek bleek de taakveld-ordering zelf aan discussie onderhevig.

Iteratief proces

Zoals eerder beschreven, is dit een iteratief proces. Dat betekent dat deze inzichten in de komende periode gaandeweg zullen worden verdiept in diverse workshops en gesprekken met beleidsmakers, en mensen van uitvoeringsorganisaties en met experts van JenV en van andere departementen en uit wetenschap en bedrijfsleven. Zodat enerzijds de analyse verdiept wordt en anderzijds gewerkt wordt aan de doelstelling van de TechAgenda, om meer mensen bewust te maken van de aankomende technologieën en zo tijdig te kunnen acteren.

Tabel 4: Technologieën in relatie tot taakvelden

Taakveld	5G/Mobile data	Quantum communicatie	Predictieve Analyse	Big-data & data-analytics	Quantum computing	Cloud en high performance grid computing	Profiling	Privacy-enhancing technologieën	Internet of Things	Immersief	Quantum sensing	Natural Language Processing	Beeldherkenning	Robotic Process Automation (RPA)	Synthetic Media	Digital security & cybersecurity	Digital identity & self-sovereign identity	Satellieten	Social media en social media analytics	Digital twins	Cryptocurrencies	Robots	Imaging technologieën (beeldsensoren)	Expertsystemen	Autonome voertuigen en systemen	Genetic engineering	Blockchain	Smart contracts	Wearables	Biochips & biosensoren	DNA-analyse
Crisisbeheersing en- bestrijding (Brandweer, deel NCTV (opsporing en Cyber apart)	4	4	3	3	3	3	3	3	3	3	3	2	3	1	3	2	2	2	3	3	2	3	2	1	3	2	2	1	1	1	1
Rechtspleging en rechtshandhaving (Recht, Rechtsbescherming, Openbaar Ministerie)	3	4	2	3	3	3	2	3	2	3	2	3	2	3	3	2	2	2	1	1	1	1	1	2	1	1	2	3	2	1	1
Preventie, handhaving en opsporing (Politie, deel NCTV)	3	4	3	3	4	3	3	3	2	3	2	3	3	3	2	2	2	2	2	2	2	2	2	1	2	1	2	1	2	2	2
Uitvoeren van straffen (coördinatie en uitvoering straffen, gevangeniswezen en CJIB)	3	2	3	3	2	2	3	3	2	2	2	1	2	3	1	1	2	3	2	1	1	2	2	1	3	2	1	1	2	2	1
Forensische opsporing (NFI)	3	3	3	3	2	2	4	2	2	2	3	2	3	1	3	2	1	2	2	1	2	1	2	2	2	4	1	1	2	3	4
Cybersecurity en cyberinvestigation (NCSC, deel politie, diensten)	4	4	4	3	4	3	1	3	4	3	3	2	1	1	3	4	3	2	2	2	2	1	1	2	1	1	1	2	1	1	1
Migratie	3	2	3	2	1	2	3	3	2	2	1	2	2	2	1	1	2	2	2	1	2	1	2	2	1	1	1	1	1	1	1
Bedrijfsvoering (gebruik technologie voor de eigen processen)	4	4	1	3	3	3	2	3	3	2	3	3	1	3	1	3	2	1	1	2	1	2	1	2	1	1	2	2	1	1	1
Totaal voor JenV	3,4	3,4	2,8	2,9	2,8	2,6	2,6	2,9	2,5	2,5	2,4	2,3	2,1	2,1	2,1	2,1	2	2	1,9	1,6	1,6	1,6	1,6	1,6	1,8	1,6	1,5	1,5	1,5	1,5	1,5

Legenda

- 1 = Weinig kansen of risico's, voor JenV zelf en/of door maatschappij
- 2 = Enige kansen en risico's, voor JenV zelf en/of door maatschappij
- 3 = Redelijk wat kansen en/of risico's, voor JenV zelf en/of door maatschappij
- 4 = Veel kansen en/of risico's, voor JenV zelf en/of door maatschappij

4. Koppeling met het Organisational readiness level (ORL)

Om te kunnen bepalen wat het meest optimale handelingsperspectief is voor JenV, is van belang om naast de positie en prioritering van de technologie, ook te kijken naar de organisatie zelf. Sommige technologieën zijn zeer urgent en impactvol, en krijgen al veel aandacht van beleidsmakers en innovatoren. Andere technologieën zijn nog een stuk minder geborgd binnen de organisatie.

De mate waarin JenV-organisaties al aandacht besteden aan een technologie wordt aangeduid met de term 'organisational readiness' en bestaat uit drie delen: (i) is er al een (interdepartementaal) ecosysteem, staat de technologie al ergens op de agenda (ii) Is de wetenschap er mee bezig; wat is er aan kennis en onderzoek uitgevoerd, al dan niet in opdracht van JenV en (iii) is er specifieke aandacht voor deze technologie binnen JenV.

Aan de hand van een beperkte set gesprekken met betrokken ambtenaren, waaronder leden van het AI team en van het vooroverleg Innovation Board is een globale analyse uitgevoerd.

Dit levert een startpunt om in de vervolgworkshops met taakvelden en domeinen op voort te kunnen bouwen, afhankelijk van de gemaakte keuzes ten aanzien van handelingsperspectief en vervolg.

Tabel 5: Organisational readiness

Netwerk/ecosysteem	Kennis/Wetenschap / onderzoek	Aanpak JenV
Is er een netwerk (operationeel, beleid, interdepartementaal, en/of binnen JenV)?	Is/wordt er onderzoek gedaan met/in opdracht van JenV?	Is er een trekker binnen JenV / is het duidelijk belegd?
Is er een gezamenlijke interdepartementale aanpak?	Is er verbinding met de wetenschap?	Is er een actieplan/ visie / strategie (lees: gecoördineerde aanpak)?
Vinden er experimenten/ innovatieprojecten plaats? Binnen de overheid, wetenschap, private partijen?	Zijn er onderzoeksrapporten beschikbaar over kansen, risico's en maatschappelijke consequenties?	Is er voldoende personele capaciteit op het onderwerp?
Is er aandacht voor de technologie in de EU of daarbuiten?		Is er kennis binnen JenV over de technologie?

Onderstaande termen zijn ieder gescoord op een aantal variabelen (drie, vier of vijf, die allemaal een score ontvingen van onvoldoende tot goed). Samen verbeelden ze het Organisational Readiness Level voor JenV-breed. In een aantal gevallen is een technologie voor een specifiek onderdeel van JenV goed in beeld, maar ligt de uitdaging in het verbreden van de betrokkenheid.

Tabel 6.1: Samenvatting Organisational Readiness Level voor cluster Digitale Veiligheid

Digital ID	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek		matig		
Aanpak JenV	onvoldoende			

Post Quantum Cryptografie	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek		matig		
Aanpak JenV		matig		

Digital Security en cybersecurity	Organisational Readiness Level			
Ecosysteem				goed
Kennis en onderzoek				goed
Aanpak JenV			voldoende	

Privacy Enhancing Technologies	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek				goed
Aanpak JenV			voldoende	

Blockchain	Organisational Readiness Level			
Ecosysteem				goed
Kennis en onderzoek				goed
Aanpak JenV		matig		

Tabel 6.2: Samenvatting Organisational Readiness Level voor cluster Artificial intelligence

Profiling	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Predictieve Analyse	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Beeldherkenning	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek			voldoende	
Aanpak JenV			voldoende	

Natural language Processing	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek				goed
Aanpak JenV		matig		

Synthetische media	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek				goed
Aanpak JenV		matig		

Beslisalgoritmen en expertsystemen	Organisational Readiness Level			
Ecosysteem	onvoldoende			
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Tabel 6.3: Samenvatting Organisational Readiness Level voor cluster Data Science

Social media en social media analytics	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek				goed
Aanpak JenV		matig		

Big data en data analytics	Organisational Readiness Level			
Ecosysteem				goed
Kennis en onderzoek			voldoende	
Aanpak JenV			voldoende	

Imaging Technologies	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek		matig		
Aanpak JenV	onvoldoende			

Robotic Process Automation	Organisational Readiness Level			
Ecosysteem		matig		
Kennis en onderzoek		matig		
Aanpak JenV		matig		

Tabel 6.4: Samenvatting Organisational Readiness Level voor cluster Netwerken en infrastructuur

Internet of Things	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Satellieten	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV			voldoende	

5G	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Cloud en high performance grid computing	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV			voldoende	

Tabel 6.5: Samenvatting Organisational Readiness Level voor cluster Digitale werkelijkheid

Virtual en Augmented Reality	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV		matig		

Wearables	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek			voldoende	
Aanpak JenV			voldoende	

Digital Twins	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek		matig		
Aanpak JenV	onvoldoende			

Tabel 6.6: Samenvatting Organisational Readiness Level voor cluster Quantumtechnologie

Quantum Computing en communicatie	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek		matig		
Aanpak JenV		matig		

Quantum Sensing en metrologie	Organisational Readiness Level			
Ecosysteem			voldoende	
Kennis en onderzoek		matig		
Aanpak JenV		matig		

5. Lessons Learned

De volgende lessen zijn geleerd uit bovenstaand iteratief proces:

1. *Grondige aanpak onderzoek naar impact, urgentie, kansen en risico's is wenselijk.*
Waar bij deze TechAgenda nog met een beperkte Delphi methode is gewerkt, is het voor de volgende iteraties aan te raden om deze uitgebreid(er) uit te zetten met eventueel een toelichting in de vorm van een filmpje of een persoonlijke toelichting om de response rate zo hoog mogelijk te maken. Daarbij werken met een interne- en externe enquête zou bevorderlijk werken voor een robuustere analyse.
2. *Er liggen kansen om nog breder gebruik maken van reeds beschikbare (tech-)scans en netwerken binnen en buiten JenV.*
3. *Het is wenselijk om definities van technologieën en het afwegingskader nader te verhelderen voorafgaand aan enquête en analyse.*
Een betere afbakening van de verschillende technologieën is niet alleen voor de respondenten van de Delphi nuttig maar ook voor JenV en voor extern gebruik.
4. *Een grotere betrokkenheid van JenV-organisaties bij de diverse analyseslagen is wenselijk.*
De TechAgenda kan nog aan kracht winnen door meer inbreng vanuit de JenV-organisaties en beleidsdirecties. Zo kan de kwaliteit van de analyses verbeterd worden, en de aansluiting op het primaire proces worden verhoogd.

Colofon

De Technologieagenda van het Ministerie van Justitie en Veiligheid biedt inzicht in de relevante technologieën voor het ministerie in de komende jaren. De agenda is tot stand gekomen met medewerking van velen binnen en buiten het ministerie van Justitie en Veiligheid. De Directie Innovatie, Kennis en Strategie heeft dit proces gefaciliteerd.

Fotografie

Mark David (cover), Tineke Dijkstra (p. 4), Paul Voorham (p. 9),
Louis Ottens (p. 10), Edwin Walvisch (p. 28)

Illustraties

Flatland

Directie X

Technologieprogramma
V1.0

April 2022