Techvisie 2.0

Kees Verhoeven

D66

Voor de toekomst

Inhoudsopgave

Samenvatting en belangrijkste voorstellen

Digitalisering is een van de grote thema's van onze tijd. Nieuwe technologieën veranderen de wereld in sneltreinvaart en dit heeft voor mensen en bedrijven onomkeerbare gevolgen, doorgaans positief, maar soms ook negatief. Technologie hoeft ons niet te overkomen, de mens kan het zelf vormgeven. Dit vraagt wel om politieke keuzes. In Nederland én in Europa. En daar kunnen we niet langer mee wachten. We laten nu te veel maatschappelijke kansen liggen. China en de Verenigde Staten streven ons voorbij. Digitalisering bedreigt onze autonomie, onze democratie en onze economie. En we zijn kwetsbaar voor buitenlandse beïnvloeding en aanvallen op onze vitale infrastructuur.

Onze visie is dat technologie kansen biedt voor welvaart en welzijn. We moeten meer doen om die kansen te grijpen. D66 wil voorkomen dat Nederland internationaal achterop raakt. We moeten actief optreden, zodat technologie onze vrijheid vergroot en eerlijk uitpakt. Dit betekent een voortdurende zoektocht naar evenwicht.

Ten opzichte van onze eerste Techvisie uit 2016[1] zijn er drie thema's die extra aandacht vragen: de impact van kunstmatige intelligentie, de macht van de grote technologiebedrijven en de dreiging van digitale aanvallen. Hier gaan we in drie aparte hoofdstukken op in. We starten deze visie met het benutten van kansen (hoofdstuk 1) en sluiten af met voorstellen voor een betere politieke organisatie van digitalisering (hoofdstuk 5).

Ons doel is dat Nederland niet achterop loopt, maar tot de digitale koplopers behoort. We werken aan een toekomst waar technologie niet uit de hand loopt, omdat de overheid reguleert waar nodig. Een toekomst waar de opbrengst van technologie niet teveel uiteen loopt, omdat de welvaart eerlijk verdeeld wordt.

[1] D66: Techvisie (2016): https://d66.nl/content/uploads/sites/2/2016/06/Techvisie-online.pdf

1. Digitale kansen beter benutten

Technologie kan de mondiale voedselproductie verbeteren en de opwarming van de aarde helpen bestrijden. Drones kunnen pakketjes bezorgen en implantaten waken in de toekomst over onze gezondheid. De mogelijkheden zijn eindeloos. Onze uitgangspositie is goed, maar Nederland laat veel kansen liggen.

In vergelijking met ons omringende of vergelijkbare landen (Canada, Israël, Singapore, Scandinavië, Duitsland, Frankrijk en het Verenigd Koninkrijk) ontbreekt het aan digitale urgentie, ambitie en een agenda. Ondanks de doorbraak van succesvolle startups zoals Adyen, Elastic en Catawiki, doen we te weinig om startups in Nederland door te laten groeien. En we investeren te weinig in onderzoek en innovatie.

De kwaliteit van het onderwijs en de zorg kunnen fors verbeterd worden met behulp van digitale technologieën. De behoeften van patiënt en leerling kunnen nauwkeuriger gemeten worden en robots kunnen de werkdruk verlagen. Dit vraagt wel om een andere rolverdeling tussen mens en machine waarbij de juiste digitale en sociale vaardigheden centraal staan.

De overheid zelf kan zijn digitale dienstverlening fors verbeteren, zonder het anoniem en onmenselijk te maken. Dat vereist een goede omgang met persoonsgegevens, identificatie, ICT-projecten, software en algoritmes. Toegankelijkheid en uitlegbaarheid horen bij de beginselen van behoorlijk bestuur.

D66 stelt voor:

- Investeer als overheid en bedrijfsleven meer in onderzoek. Herzie verouderde regels die innovatie belemmeren. Maak het voor startups beter mogelijk om kennismigranten aan te trekken en om salaris in aandelen uit te betalen.
- Geef digitale systemen (robots, chips, games, virtuele hulp) een structurele plek in het onderwijs en de zorg. Stel de juiste digitale en sociale vaardigheden centraal in het onderwijs en op de lerarenopleiding. Maak omscholing en bijscholing voor iedereen mogelijk.
- Stel als overheid de menselijke behoefte centraal. Wees transparant en terughoudend met datagebruik, volgens de één-bron-gedachte. Organiseer ICT-projecten kleinschaliger en zoveel mogelijk op basis van open source. Maak algoritmes en datasets toetsbaar en hun besluiten omkeerbaar.

2. Kunstmatige intelligentie positief inzetten

De meest ingrijpende technologie van dit moment is kunstmatige intelligentie (KI), waarbij apparaten reageren op data of impulsen en zo zelfstandige beslissingen nemen. Door big data, supercomputers, cloudopslag en het internet der dingen neemt KI een vlucht die alle sectoren en beroepen raakt.

De potentie van KI neemt drie uitdagingen met zich mee. Allereerst een mondiale concurrentieslag waarbij China en de VS Europa voorbij dreigen te streven. Ten tweede het uithollen van grondrechten, burgerrechten en maatschappelijke waarden. En ten derde verandering en mogelijk verlies van werkgelegenheid, met als risico toenemende tweedeling.

Dit complexe samenspel leidt al snel tot felle debatten en polarisatie. D66 kiest voor een gebalanceerde benadering: betere KI-opleidingen en fors meer investeren in KI-kansen, maar tegelijk reguleren op basis van ethische principes en waar nodig welvaart herverdelen.

D66 stelt voor:

- Breng de capaciteit van het KI-onderwijs en het wetenschappelijk onderzoeksbudget fors omhoog: in 2022 naar 1.000 studenten en 500 miljoen euro per jaar.
- Formuleer Nederlandse KI-principes en eisen die het gebruik van KI richting en begrenzing geven. KI moet eerlijk en sociaal zijn. Dwing transparantie en uitlegbaarheid af en maak correctie en compensatie mogelijk. Stel een algoritme-waakhond in, die toezicht houdt op de inzet van algoritmes (en onderliggende datasets).
- Zorg dat iedereen toekomstige –digitale, sociale en creatieve- vaardigheden aanleert. Verdeel als overheid de toekomstige welvaart. Het belasten van kapitaal, een basisinkomen of mede-eigendom van machines voor werknemers zijn opties.

3. De datamacht van techreuzen inperken

Net als de drie voorgaande revoluties heeft ook de vierde revolutie zijn eigen machthebbers gecreëerd. De techreuzen Amazon, Facebook, Google, en Apple zijn de grote industrialisten van onze tijd. Door hun omvang heeft hun machtspositie economische, persoonlijke, creatieve, sociale en democratische gevolgen.

Zo beperken ze de keuzevrijheid en privacy van gebruikers, smoren ze concurrentie in de kiem, onderbetalen ze kleine zelfstandigen en werknemers, ontlopen ze belasting en doen ze te weinig tegen de verspreiding van desinformatie en nepnieuws. Het aanpakken van deze problemen is een praktische noodzaak, maar het inperken van de datamacht van de techreuzen is ook een democratisch principe. Macht vereist tegenmacht.

Politici vinden het ingewikkeld om deze grenzeloze bedrijven aan te pakken, maar het is wel nodig, zowel op nationaal als Europees niveau. D66 kiest als hoofdroute het mededingingsrecht, omdat we de marktmacht *zelf* willen betwisten en niet enkel de *gevolgen* ervan willen bestrijden. Daarnaast zetten we in op privacywetgeving, het auteursrecht en belastingheffing.

D66 stelt voor:

- Pas de relevante artikelen uit het Europees Verdrag en de Nederlandse Mededingingswet aan. Geef data zo een plek in mededinging, treed strenger op tegen marktmacht en knip bedrijven desnoods op[2]. Stel een Europese toezichthouder voor mededinging in.
- Zorg voor strikte naleving van de Europese privacywet AVG. Informeer burgers actief over hun recht tot regie over hun persoonsgegevens. Geef mensen het recht geen data te delen, met behoud van toegang tot de dienst. Toets gezichtsherkenning (en Virtual Reality/Augmented Reality) vooraf op hun privacy-consequenties.
- Voer de druk in de Europese Raad op zodat de Europese digitaks er zo snel mogelijk komt en voer het anders zelf in. Bescherm auteurs en makers beter via het auteursrecht, maar niet via een linktaks of uploadfilter.

[2] D66 dient hiertoe een initiatiefnota in

4. Digitale aanvallen afslaan

Cybersecurity wordt steeds belangrijker omdat onze samenleving steeds afhankelijker is van digitale technologie. Tegelijk neemt de digitale dreiging toe, in de vorm van desinformatie, hackaanvallen en economische spionage. Een technologische wapenwedloop en zelfs *cyberwarfare* zijn reële toekomstscenario's.

Het is de verantwoordelijkheid van de overheid om onze democratie, onze vitale infrastructuur, onze bedrijfsgeheimen en onze staatsveiligheid te beschermen. Dit zonder te vervallen in censuur, zonder onverantwoord gebruik van cyberwapens en zonder lukraak bedrijven uit bepaalde landen te weren.

D66 stelt voor:

- Organiseer een bewustwordingscampagne voor de twee verkiezingen in 2019 en onderzoek de impact van desinformatie. Dwing af dat de afzender van advertenties altijd duidelijk is en dat trollen, bots en nepaccounts actiever worden geweerd.
- Maak een wettelijk afwegingskader voor cyberwapens op basis van zeroday-exploits[3]. Verzwak encryptie niet voor opsporingsdoeleinden. Verplicht grote bedrijven een hoofdstuk in hun jaarverslag te wijden aan cybersecurity. Scan de vitale infrastructuur op kwetsbaarheden en verouderde software (legacy) en beloon ethisch hackers beter.
- Formuleer een Nationaal Technologie Kader bestaande uit een risicoanalyse en een eisenpakket (zoals audits toestaan en broncodes vrijgeven) voor alle buitenlandse leveranciers van onderdelen in de Nederlandse vitale infrastructuur. Ontwikkel tevens een Europese Technologie-Strategie en benoem daarin technologieën die we als Europa in eigen hand moeten houden.
- Zet in VN-verband in op een digitale uitwerking van de Geneefse conventies, in lijn met de Tallinn manual 2.0 over internationaal recht in de cyber context. Zet ook in op het voorkomen van een KI-wapenwedloop met killer robots en onbemande drones.

[3] D66 dient hiertoe een initiatiefwet in.

5. Digitalisering borgen in bestuur en politiek

Het is de overheid, van lokale politiek tot de Europese Commissie, die digitale technologie in goede banen moet leiden. De Tweede Kamer speelt hierin een belangrijke rol. Om deze rol goed te kunnen vervullen moet voldaan worden aan bepaalde randvoorwaarden.

Allereerst vraagt dit het in huis halen van de nodige kennis en expertise. Ten tweede moeten kabinet en Kamer zelf het goede voorbeeld geven op digitaal vlak. Ten derde moet het politieke debat, het bestuur en de wetgeving beter georganiseerd worden. Dit begint met een overkoepelende agenda en goede coördinatie in plaats van de huidige versnippering binnen zowel kabinet, parlement als in de organisatie van advies en toezicht.

D66 stelt voor:

- Stel een hoge Digitale Autoriteit in, direct onder minister-president. Deze bestrijkt de digitale overheid, de digitale economie, de digitale veiligheid en digitale ethiek. Het alternatief is een minister voor Digitale Zaken in het eerstvolgende kabinet.
- Stel nog deze Kamerperiode een Vaste Kamercommissie Digitale Zaken in. Vergelijkbaar met de Vaste Kamercommissie Europese Zaken. Doe als presidium van de Tweede Kamer onderzoek naar de mogelijkheid van versnelde wetgevingstrajecten.

Techvisie 2.0: een politieke agenda voor de digitale toekomst

Digitale technologieën veranderen de wereld sneller dan ooit. Ze veranderen de manier waarop docenten lesgeven, hoe dokters en patiënten met elkaar praten, waar politici over debatteren en hoe mensen nieuws delen. Achter de schermen werken algoritmen en kunstmatige intelligentie op manieren die onze hersenen niet eens meer herkennen. Onze samenleving wordt op deze manier compleet anders ingericht. Hand in hand met globalisering verandert digitalisering onze leefomgeving en onze samenleving. Aan onze fysieke wereld wordt letterlijk een digitaal landschap toegevoegd.

Dat dit voor mensen en bedrijven onomkeerbare gevolgen heeft, doorgaans positief maar soms ook negatief, is inmiddels duidelijk. Nieuwe producten, diensten en mogelijkheden doen hun intrede, verouderde systemen worden vervangen of verdwijnen gewoon. Verhoudingen veranderen en er ontstaan nieuwe kansen en nieuwe dilemma's. Bovendien zijn de sociale, culturele en economische consequenties moeilijk te overzien en onvoorspelbaar.

Samen met de opwarming van de aarde is de voortdurende digitalisering van onze samenleving het grote thema van deze tijd. Het verandert ons dagelijks leven, onze manier van communiceren, onze veiligheid, onze waarden en onze democratie. Maar de abstracte vorm, grote snelheid en de onbekende bestemming van digitalisering maken dat de politiek relatief weinig doet. Terwijl bij gevestigde thema's verdeeldheid vaak in de weg staat, is hier een gebrek aan kennis en overzicht het grootste probleem. Digitalisering lijkt haast te groot, technisch en complex om aan te pakken. Dit terwijl digitalisering juist om politieke keuzes vraagt.

Politiek is aan zet

Die politieke keuzes moeten we nu maken. Afwachten en hier en daar een halve ingreep plegen is in 2019 geen optie meer. We moeten de kansen van digitalisering voor het bedrijfsleven, de landbouw, het onderwijs, de zorg en de overheid veel beter benutten. Tegelijk leiden nieuwe technologieën vandaag en morgen tot maatschappelijke uitdagingen die een politiek antwoord behoeven. Zoals besluitvorming door algoritmes en het verdwijnen van menselijke banen door automatisering. Of de concentratie van data en macht bij een klein aantal grote bedrijven. Of de beïnvloeding van onze democratie en de aanval op onze vitale infrastructuur. Steeds geldt: de politiek is aan zet. Waar nodig nationaal, waar mogelijk Europees of internationaal.

Daarom heeft D66 een Techvisie 2.0 opgesteld: een politieke agenda voor de digitale toekomst. Onze Techvisie 1.0 uit 2016 is inmiddels toe aan vernieuwing. Het doel was destijds meer politieke aandacht en publiek geld voor digitalisering. Deels is dit via het regeerakkoord gelukt, deels is de analyse van toen ingehaald door de razendsnelle veranderingen. Een update was nodig. Hierin is onze hoofdanalyse dat de huidige dynamiek van digitalisering actiever politiek handelen vereist. In het kort is onze visie daarbij dat technologie kansen biedt voor de toekomst en dat we voorop moeten lopen om die kansen te grijpen. Het risico van achterlopen is namelijk te groot. Tegelijkertijd moeten we inzien dat technologie ook negatieve aspecten meebrengt. We moeten zorgen dat technologie vrijheid vergroot in plaats van verkleint. Technologie moet menselijk en eerlijk uitpakken.

Dat werken we uit langs vier lijnen. Allereerst het benutten van kansen om iedereen te laten profiteren. Ten tweede een evenwichtige benadering van kunstmatige intelligentie, waarbij we inzetten op investeren, reguleren en herverdelen. Ten derde het controleren van de datamacht van grote techbedrijven en digitale platforms. Ten vierde het beschermen van onze democratie en infrastructuur tegen digitale inmenging en aanvallen van buitenaf. Tot slot zetten we uiteen wat de politiek moet doen om grip te krijgen op digitalisering.

Visie: digitale technologieën in een menselijke samenleving

Digitale technologieën hebben ons veel gebracht.

- Het heeft snel sociaal contact en zakelijke communicatie op afstand mogelijk gemaakt: chatdiensten, e-mail.
- Het heeft saaie en zware arbeid verlicht: automatisering, robotisering.
- Het heeft handige, leuke en spannende diensten opgeleverd: muziek- en videodiensten, digitale televisie, games.
- Het heeft grote hoeveelheden informatie voor iedereen en overal toegankelijk gemaakt: websites, zoekmachines, smartphone-apps.
- Het heeft economische transacties verbeterd en veiliger gemaakt: webshops, online bankieren.
- Het heeft bijgedragen aan zelfontplooiing en inspraak: social media, platforms.

De verdere mogelijkheden lijken haast oneindig. Dankzij digitalisering en nieuwe technologische toepassingen kunnen we in de toekomst gezonder en ouder (en wellicht zelfs onsterfelijk) worden, kunnen we klimaatverandering aanpakken, de voedselvoorziening verbeteren, ziektes voorkomen, doelgerichter leren, plezieriger wonen in slimme steden, sneller reizen zonder ongelukken, effectiever en schoner produceren, prettiger en veiliger werken en relaties aangaan met iedereen in de wereld (desnoods een robot).[4] Toepassingen van kunstmatige intelligentie, quantumcomputing, fotonica, blockchain en robotica bieden grote mogelijkheden voor Nederland om de productiviteit van bedrijven en de kwaliteit van de maatschappelijke dienstverlening te laten stijgen.

Weliswaar heeft de overheid aan deze voordelen en kansen een financiële bijdrage geleverd via publieke investeringen in onderzoek en innovatie.[5] Tegelijkertijd heeft de overheid zich relatief op afstand gehouden. Soms terecht, zoals bij de ontwikkeling van internetprotocollen. Soms niet terecht, waardoor het internet een ongereguleerde ruimte is geworden.

Digitalisering was aanvankelijk helemaal geen politiek onderwerp en toen het na de eeuwwisseling langzaam op de politieke agenda kwam lag de focus vooral op het benutten van economische kansen. Optimisme voerde de

[4] In zijn boek “De wereld van morgen” (2017) schetst futurist Richard van Hooijdonk de digitale toekomst, “die te mooi is om waar te zijn”. Het was een van de bronnen die ik veel heb geraadpleegd bij hoofdstuk 1 over kansen (in het onderwijs en de zorg).
[5] Veel mensen vergeten dit feit maar hoogleraar innovatie-economie Mariana Mazzucato heeft hier in haar boek “De Ondernemende staat” (2015) scherp op gewezen.

boventoon en dat was ook begrijpelijk, want Sillicon Valley wist hoe ze haar prachtige producten en diensten moest verkopen.

Naast kansen ook bedreigingen

Lang bleven de bedreigingen van nieuwe technologieën onderbelicht of we zagen ze niet op tijd aankomen. Inmiddels krijgen de maatschappelijke nadelen steeds scherper gestalte. Elke politicus die zijn ogen daarvoor sluit, verzaakt zijn morele plicht om mensen te beschermen tegen onwenselijke veranderingen en om de onzekerheid om te zetten in hoop en perspectief voor iedereen. Historicus Philipp Blom wijst erop dat vooruitgang niet doelgericht hoeft te zijn, dat digitalisering niet hoeft te verlopen als eerdere industriële revoluties, dat er steeds meer verliezers zijn en dat technologie ook de eigen mogelijkheden en verantwoordelijkheden van mensen inperkt[6].

Wat zijn dan die nadelen en bedreigingen? We noemen er een aantal om het concreet te maken.

1. Allereerst de ondermijning van burgerrechten (naast privacy ook gelijkheid en vrijheid) omdat bedrijven en overheden steeds meer persoonsgegevens van burgers verzamelen. Via het internet wordt met deze gegevens geknutseld door grote rekenkracht en slimme algoritmes.
2. Ten tweede de moderne monopolies in de digitale *winner-take-all-economie* die creativiteit, concurrentie en innovatie uithollen met moeilijk te doorgronden verdienmodellen, gebaseerd op dataprofielen en advertentie-verkoop.
3. Ten derde de statelijke actoren die desinformatie en polarisatie verspreiden via social mediaplatforms en die digitale aanvallen plegen op energienetwerken, ziekenhuizen en betalingssystemen (of deze mede veroorzaken zoals bij Wannacry[7]). Ook is er het risico van infiltratie via technologiebedrijven[8]
4. Ten vierde zijn er uitdagingen op de langere termijn zoals stijgend energieverbruik en verdwijnende banen door automatisering. Met als mogelijk gevolg een toenemende afstand tussen een digitale kopgroep, en een groeiende groep afhakers.

Dit hoeven geen onvermijdelijke veranderingen te zijn. Technologie hoeft ons niet te overkomen. Maar als we het politiek niet voldoende bijsturen en begrenzen dan wordt het voor veel mensen niet meer te bevatten. Naast de morele opdracht om mensen voldoende te beschermen, welvaart eerlijk te verdelen en hoop te bieden, is het ook

[6] Philipp Blom: "Wat op het spel staat" (2017), p 57-64
[7] Zie: https://www.nrc.nl/nieuws/2017/05/14/wannacry-kwam-bij-de-nsa-vandaan-9075218-a1558565
[8] De discussie hierover spitst zich toe op Kaspersky Antivirus, Huawei en Hytera Mobilfunk, maar speelt breder. Hoe dan ook dienen we verder te kijken dan China en Rusland. Fox-IT verzorgt cryptografie voor de Nederlandse overheid maar is onderdeel van een Brits bedrijf, dat na Brexit dus ook van buiten EU komt.

een praktische keuze. Want als we de nadelen, bedreigingen en onzekerheid niet voldoende wegnemen of compenseren dan verdampt het vertrouwen en verdwijnt het (democratische) draagvlak voor technologie. En dat betekent ook dat bijvoorbeeld investeringen in de kansen en mogelijkheden niet meer op steun van de bevolking kunnen rekenen.

D66 leidt niet aan technologische somberheid maar technologisch ontwikkelingen dwingen ons wel te blijven nadenken over de gevolgen van digitalisering. Door de commerciële mechanismen die erachter zitten, is de gedachte dat de markt digitalisering wel in goede banen leidt een denkfout. En de stelling dat mensen zelf verantwoordelijk zijn voor positieve digitalisering is slechts deels waar. Dus ondanks haar structurele voorkeur voor de korte termijn, haar toenemende afkeer van complexiteit, haar trage besluitvorming en haar matige track record met ICT moet de overheid haar verantwoordelijkheid nemen. In die zin heeft Sidney Vollmer[9] gelijk als hij schrijft dat "de samenleving zich technologieën niet simpelweg ten nutte maakt door eraan te wennen maar door reguleringssystemen in te voeren".

[9] Sidney Vollmer: ON/OFF (2017), p. 166

De visie van D66

Ja, D66 wil technologie omarmen en benutten voor een betere samenleving. Daarbij moeten we in het bijzonder oog hebben voor de digitale concurrentiestrijd waarbij Europa het dreigt af te leggen tegen enerzijds het techkapitalisme van de Verenigde Staten en anderzijds de staatstechnologie uit China. Cijfers over R&D investeringen, intellectueel eigendom en wetenschappelijke publicaties wijzen hierop. Net als het feit dat van de twintig grootste internetbedrijven ter wereld er 11 uit de VS komen, 9 uit China en geen enkele uit Europa.

Figuur 1: Internetbedrijven naar marktwaarde (2018)

Rank			Market Value ($B)	
2018	Company	Region	5/29/13	5/29/18
1)	Apple	USA	$418	$924
2)	Amazon	USA	121	783
3)	Microsoft	USA	291	753
4)	Google / Alphabet	USA	288	739
5)	Facebook	USA	56	538
6)	Alibaba	China	--	509
7)	Tencent	China	71	483
8)	Netflix	USA	13	152
9)	Ant Financial	China	--	150
10)	eBay + PayPal*	USA	71	133
11)	Booking Holdings	USA	41	100
12)	Salesforce.com	USA	25	94
13)	Baidu	China	34	84
14)	Xiaomi	China	--	75
15)	Uber	USA	--	72
16)	Didi Chuxing	China	--	56
17)	JD.com	China	--	52
18)	Airbnb	USA	--	31
19)	Meituan-Dianping	China	--	30
20)	Toutiao	China	--	30
		Total	$1,429	$5,788

Bron: Kleiner Perkins Internet Trends

Nee, D66 wil niet op de rem staan of teruggaan in de tijd. Maar we moeten ons ook niet neerleggen bij de onvermijdelijkheid van technologische verandering en machteloos toekijken. De politiek moet digitale technologie laten bijdragen aan een menselijke maatschappij met sociale samenhang. De grootste belofte van technologie is altijd vooruitgang en verbetering geweest. Zo beloofde het internet mensen dichterbij elkaar te brengen, vrijheid te vergroten en macht te decentraliseren. Dat is grotendeels gelukt, maar tegelijk is er de dreiging van polarisatie in plaats van verbinding, controle in plaats van vrijheid en centralisatie in plaats van decentralisering van macht. Ook eigenaren van huidige en toekomstige technologieën zullen bepaalde beloftes niet nakomen of schaduwkanten ontkennen. Dan moet de politiek durven in te grijpen en zorgen voor een goede balans.

Ons doel is een land waar mensen de regie hebben over technologie. Tegelijkertijd moeten bedrijven in staat zijn kansen te benutten. En moet de overheid innovatie stimuleren, burgerrechten waarborgen, concurrentie bevorderen, tegenwicht geven aan datamacht en mensen beschermen tegen digitale aanvallen. De inzet is een land dat niet achter loopt, maar dat tot de digitale koplopers behoort door voldoende te investeren. Een land waar technologie niet uit de hand loopt omdat de overheid weet wanneer te reguleren. En een land waar de opbrengst van technologie niet teveel uiteen loopt, omdat de overheid zorgt voor een eerlijke verdeling van de welvaart.

Hoofdstuk 1. Digitale kansen beter benutten

Technologie maakt op vele vlakken verbetering mogelijk. Digitalisering kan de mondiale voedselproductie verbeteren of de opwarming van de aarde helpen bestrijden. Dichterbij huis kun je denken aan slimme steden die schoner en veiliger zijn, zelfrijdende voertuigen zonder ongelukken, drones die pakketjes bezorgen of huishoudens die zelf energie opwekken.

Nederland laat echter nog veel kansen liggen.

Als zorg-innovatie net zoveel politieke aandacht had gekregen als het eigen risico, dan zouden we een stuk verder zijn geweest met betere en betaalbare zorg. Hetzelfde geldt voor onderwijsinnovatie en klimaatinnovatie. Het debat focust zich te vaak op de bestaande tegenstellingen in plaats van te kijken naar nieuwe mogelijkheden.

Het gaat vaak over de bedreigingen maar het laten liggen van kansen is juist de grootste bedreiging. Daarom zetten we in dit hoofdstuk uiteen wat de grootste verbeterkansen van digitalisering zijn in de landbouw, het onderwijs, de zorg en de overheid zelf.

Bedrijfsleven

Wereldwijd gezien heeft Nederland een excellente digitale infrastructuur. We hebben een snel en wijdverspreid internet en het grootste internetknooppunt ter wereld[10]. Ook hebben we veel slimme en 'tech-bekwame' mensen. Daarmee hebben we een goed digitaal vestigingsklimaat. Tegelijkertijd is de mondiale concurrentie (China en de VS) moordend. Als Nederland een digitale koploper wil blijven, moeten we meer investeren in zowel onze digitale infrastructuur als in onze onderzoeks- en innovatiekracht.

Hoewel continuïteit juist bij innovatiebeleid cruciaal is, en hoewel het topsectorenbeleid de afgelopen zeven jaar voor verbeterde samenwerking binnen de 'gouden driehoek' (onderwijs, bedrijven, overheid) heeft gezorgd, is de aangekondigde focusverlegging van traditionele bedrijfstakken naar maatschappelijke thema's (voedselproductie, vergrijzing, klimaatverandering) en sleuteltechnologieën (kunstmatige intelligentie, fotonica, quantumcomputing) van groot belang.

[10] De AMS-IX. Ook komen 11 van de 15 trans-Atlantische internetkabels via de Noordzeekust aan land in Europa. Dit verklaart mede de grote aantrekkingskracht van Nederland op datacenters.

Tegelijk wijzen critici op belangrijke tekortkomingen. Volgens TomTom-topman Goddijn is Europa te naïef op technologiegebied, is er een gebrek aan ambitie en slagen we er onvoldoende in om wetenschappelijk onderzoek te vertalen naar succesvolle ondernemingen[11]. In haar advies aan Economische Zaken wijst de Nederlandse Academie voor Technologie en Innovatie (ACTI)[12] op de noodzaak van meer missie-gedreven onderzoek, een betere vertaling van technologische kennis naar marktsucces (valorisatie)[13], extra onderwijs-investeringen in bèta en techniek en meer middelen voor specifieke innovatie-instrumenten en doelgerichte onderzoeksprogramma's.

Innovatie komt vooral van nu nog kleine, maar snelgroeiende bedrijven. Deze bedrijven hebben vaak een sterke vraag naar gespecialiseerd en hoogopgeleid personeel dat niet altijd te vinden is in Nederland. Daarnaast kunnen ze in vroege fases van hun ontwikkeling niet altijd concurrerende lonen betalen. Ook de toegang tot innovatieregelingen voor het innovatieve mkb, startups en scale-ups kan beter.

Een ander probleem is het voldoen aan regelgeving, zoals de Europese privacywet AVG, die digitalisering in goede banen moet leiden. Bij grotere bedrijven ontstaat daarbij een afvinkcultuur waarbij iets in orde is als "compliance zegt dat het goed is". Dit terwijl veel startups juist niet aan de compliance-last kunnen voldoen. Hiermee ontstaat in markten een barrière tot toetreding. Overigens zijn er ook startups waarbij het bedrijfsmodel bestaande reguleringen ontwijkt, waardoor ze juist een concurrentievoordeel hebben. Met het oog op deze verschillen streeft D66 naar een digitale markt die voor alle bedrijven goed werkbaar is.

D66 stelt voor:

- **Zorg voor een totaal-digitaal vestigingsklimaat met als basis: toekomstgerichte regelgeving, een expat-vriendelijke arbeidsmarkt, goed bèta-onderwijs, een sterke digitale mainport, overal snelle verbindingen en hoge connectiviteit.**
- **Kies voor meer specifieke innovatie-financiering en onderzoeksprogramma's met een concreet maatschappelijk doel. De verhouding tussen generieke (fiscale) innovatiemiddelen en specifieke instrumenten is nu ongeveer 90:10.**
- **Versoepel in de kennismigrantenregeling de looneisen voor jonge bedrijven. Zodat kleine bedrijven makkelijker kennismigranten kunnen aantrekken.**

[11] Volkskrant, 29 december 2018
[12] ACTI: "Professionalisering van de Gouden Driehoek" (2018)
[13] In de VS krijgen de beste fundamentele wetenschappers niet alleen alle onderzoeksruimte maar ook ondersteuning bij de transfer van technologie naar product.

- Bied startende bedrijven de mogelijkheid om werknemers in aandelen of opties te betalen, bijvoorbeeld door belastingheffing over uitgekeerde aandelen uit te stellen.
- Geef datacenters toegang tot groene stroom zodat alle grote spelers hun hoge duurzaamheidsdoelen kunnen waarmaken. Een ambitieus klimaatakkoord is ook van belang voor ons digitale vestigingsklimaat.
- Kijk bij regelgeving naar de praktische toepasbaarheid voor burgers en bedrijven[14]. Geef bedrijven met nog beperkte hoeveelheden klanten en/of omzet lichtere verantwoordingskaders.
- Geef nieuwe toetreders op bestaande markten snel helderheid op het gebied van wet- en regelgeving. Creëer een *level playing field*, zonder innovatie te remmen. Stel als overheid technologie-neutrale eisen: zoveel mogelijk wat in plaats van hoe.

Landbouw

Nederland is wereldberoemd om haar voedselproductie en landbouwtechnologie. Toch is de focus op economische efficiëntie te groot. De negatieve gevolgen van voedselproductie voor de leefomgeving, het milieu en dierenwelzijn worden niet meegerekend in de prijs. Daarom is het tijd voor een ingrijpende omslag in de voedselproductie. Deze transformatie wordt aangejaagd door digitalisering in de vorm van dataverzameling, gegevensanalyse en ondersteuning bij het maken van beslissingen.

Kader 1: Robots en autonome landbouwmachines bewerken 24/7 het land, zijn veel zuiniger en lichter dan de huidige grote voertuigen. De robots zijn elektrisch aangedreven, waardoor ze minder vervuilende uitstoot produceren. Ze zorgen daarbij voor een hogere opbrengst, en een lager gebruik van bestrijdingsmiddelen vanwege de precisie. Met behulp van Precision Livestock Farming (PLF) wordt via robots het gedrag van een dier continu waargenomen en geïnterpreteerd. Dit stelt het dier centraal en biedt een wereld aan mogelijkheden wat betreft tracking, tracing en dierenwelzijnsmonitoring. Landbouwdrones kunnen de percelen gemakkelijk scannen, onderzoeken en besproeien.

Ook de mogelijkheden voor het gebruik van big data in de agrosector zijn groot. Door sensoren op allerlei apparaten op het agrobedrijf en daarbuiten digitaal met elkaar te verbinden, komen enorme hoeveelheden data en dus waardevolle informatie beschikbaar. Een andere kans voor de landbouw is informatie uit de ruimte. Vanuit de ruimte brengt het Nederlands ruimtevaartbedrijf Vandersat precies bodemvocht en de watercontent van vegetatie in kaart. Door deze kennis hoeven boeren minder vaak pesticiden of kunstmest te gebruiken. Ruimtevaart is ook cruciaal vanwege satellietnavigatie. GPS (of Galileo) stuurt tractors en machines aan, ook wel

[14] Voorbeelden die vaak genoemd worden zijn de verschillende meldplichten en het feit dat bedrijven in ‘ vitale sectoren’ aan hogere eisen moeten voldoen

handsfree farming genoemd.

Kader 2: In de melkveehouderij kan data over diergezondheid gecombineerd worden met data over de melkkwaliteit en de uitstoot van broeikasgassen. Met een dergelijk totaalplaatje worden betere beslissingen gemaakt. In de koelvers-keten zorgen big data-technologieën voor de gekoelde distributie van producten. Er hoeft namelijk minder energie verbruikt te worden en voedsel bederft minder snel. Met een early-warning-systeem voor bacteriën kan bij vleesverwerkers betere kwaliteitscontrole ontwikkeld worden: goed voor de voedselveiligheid.

Nederland produceert en exporteert kassen over de hele wereld. Door moeilijk te achterhalen bouwvoorschriften en verschillende klimaatomstandigheden is het vaak lastig om tot een optimaal ontwerp te komen. Hightech rekenmodellen kunnen precies aangeven tegen welke omstandigheden een ontwerp bestand moet zijn. Dit gebeurt op basis van wereldwijde meteodata en de GPS-locatie van de nieuwe kas. Zo worden kassen nog duurzamer.

Kansen en mogelijkheden zijn er genoeg maar het benutten van deze technologieën gebeurt op te kleine schaal. Via subsidieregelingen en wet- en regelgeving kan de overheid een belangrijke aanjager zijn.

D66 stelt voor:

- Geef boeren die voorop lopen in het verminderen van milieuvervuiling meer subsidie. Richt alle landbouwsubsidies op het verduurzamen van de landbouw, met oog voor de leefomgeving, het dierenwelzijn, en de natuur.
- Laat de minister van Landbouw, Natuur en Voedsel landbouwinnovaties van Hollandse bodem internationaal onder de aandacht brengen.
- Neem alle wettelijke belemmeringen die verduurzaming van de landbouw in de weg staan weg, mits de voedselveiligheid niet in het geding komt.
- Stimuleer een cultuurverandering onder boeren die ruimte geeft voor een nieuwe generatie hightech boeren.

Onderwijs

Ieder kind heeft recht op onderwijs dat aansluit bij zijn of haar talenten en dat een goede voorbereiding is op de 21e eeuw. Digitalisering biedt de kans om het onderwijssysteem te vernieuwen, verbeteren en nauwer aan te sluiten bij de specifieke behoeftes van leerlingen. Daartoe moeten alle scholen in Nederland toegang hebben tot snel internet en voldoende ICT-middelen. Daarnaast moeten leraren voldoende tijd en (digitale) vaardigheden hebben. De regio en de omvang van de school mogen daarbij geen verschil maken.

Digitale leermiddelen kunnen de werkdruk in het onderwijs verlagen, bijvoorbeeld via adaptieve leerprogramma's. Door automatisch toetsen na te kijken, door administratie te vereenvoudigen en door gebruik te maken van systemen die handmatige processen overnemen[15]. Daarnaast bieden digitale leermiddelen de mogelijkheid voor leerlingen om te leren op een manier die bij hen past en om leerstof vanuit de hele wereld benutten.

Wat D66 betreft is ICT en informatica basisgereedschap voor iedereen. Of je nu werkt in de kunst, mode, zorg, taalwetenschap of rechtspraak, het digitale tijdperk vraagt om nieuwe vaardigheden en een (leven lang) lerende mens. Beroepen verdwijnen en verschijnen, behoeftes van werkgevers en ondernemers veranderen en diploma's zijn steeds minder een succesfactor op de arbeidsmarkt. Het gaat enerzijds meer om nieuwe vaardigheden als coderen en programmeren en anderzijds om de combinatie van rekenen, schrijven en talen spreken met *soft skills* als veerkracht, creativiteit en samenwerking. Onderwijs dient vooral om vaardigheden aan te leren die overdraagbaar zijn tussen sectoren en die helpen tijdig nieuwe specifieke kennis en kunde op te doen. Het is van groot belang dat het onderwijs beter aansluit op de arbeidsmarkt van de toekomst.

D66 stelt voor:

- **Zorg dat alle scholen binnen vijf jaar een snelle internetverbinding hebben. Dit kan door het Surfnet-model uit te breiden naar basis- en voortgezet onderwijs. Organiseer de aanwezigheid van slimme onderwijsmiddelen en toegang tot multimedia in elke klas. Weer indien nodig mobiele telefoons uit de schoolklas.**
- **Stimuleer open leerplatformen. Zodat scholen niet afhankelijk zijn van één of twee commerciële onderwijs- en leerplatformen.**

[15] Kennisnet: https://www.kennisnet.nl/artikel/werkdruk-verminderen-met-ict/

- Geef digitale leermiddelen zoals virtuele hulpprogramma's en games een plek binnen het onderwijs. Zonder persoonlijke begeleiding te vervangen. Bied gecertificeerde MOOC's (massive open online courses) aan tegen betaalbare tarieven.
- Geef elke nieuwe leraar op de lerarenopleiding voldoende digitale lesvaardigheden mee. Bied zittende leraren digitale bijscholing aan. Inclusief kennis over de privacy-risico's bij het gebruik van diensten en platforms, zoals Facebook.
- Maak de leerlijn digitale geletterdheid (inclusief computational thinking, informatievaardigheden en ICT basisvaardigheden) onderdeel van het basiscurriculum. Betrek ook mediawijsheid, nepnieuws herkennen, online privacy en cyberpesten hierbij.
- Versterk het MBO als nationale hofleverancier van technici. Doelgerichte specialisatie en duaal leren (bijvoorbeeld via practoraten) maken dit mogelijk.
- Geef iedereen toegang tot "Digitale inburgering": bijscholing die alle burgers helpt bij hun deelname aan de digitale wereld.
- Geef elke Nederlander een belastingkrediet: een bedrag dat hij/zij aan belasting zou moeten betalen dat inzetbaar is voor bijscholing aan een universiteit of hogeschool.
- Neem een voorbeeld aan Duitsland waar werkgevers, onderwijs en vakbonden investeren in opleidingen voor vakkrachten, waarbij werkgevers als sector collectief mee-investeren en waar ze werken met *WeiterbildungsMasters*, praktijkgerichte parttime Masters voor mensen die al werken en nieuwe vaardigheden willen leren.

Kader 3: Het tekort aan technici op de arbeidsmarkt is de afgelopen jaren gestegen en zal blijven stijgen met een aantrekkende arbeidsmarkt. Dit vraagt om een aanvalsplan. Zowel overheid als werkgevers hebben fondsen voor omscholing. Deze fondsen kunnen veel beter op elkaar worden aangesloten. Met name in de technische sector. Ook kunnen vaker samenwerkingsverbanden tussen rijk, gemeenten en bedrijfsleven gevormd worden. Een goed voorbeeld hiervan is het 'Masterplan Techniek', hierbij sloegen bedrijven en de gemeente Amsterdam de handen ineen. Ze proberen de kwaliteit van en instroom naar technische Mbo-opleidingen te verbeteren. Het Masterplan richt zich op: het omscholen van zij-instromers; kwaliteitsverbetering van technische opleidingen; en jongeren enthousiasmeren voor technisch onderwijs. Dit doet de gemeente samen met onderwijs en bedrijfsleven[16]. Daarnaast kan de samenwerking tussen scholen en bedrijven veel verder gaan dan stageplekken en gastcolleges. Het Techniekcollege in Rotterdam is een van de voorbeelden in Nederland waar dit te zien is.

[16] NRC: "Help, er zijn geen technici meer" (18 mei 2018).

Zorg

De afgelopen jaren zijn de zorgkosten in Nederland doorgestegen. Tegelijkertijd klagen veel mensen over de kwaliteit en de toegankelijkheid van onze zorg. Onderbelicht in het zorgdebat is de bijdrage die innovatie en technologie kunnen leveren aan betere (en goedkopere) zorg.

Digitale zorg (*E-health*), zoals Connected Care van Philips maakt het mogelijk om met sensoren op afstand patiënten te monitoren en preventie te verbeteren via zelfdiagnose. Mits de medische gegevens juridisch goed beschermd zijn, kan een computer als eerste de foto's of scans analyseren en verdachte plekken markeren, of fungeren als second opinion naast de specialist. Supercomputers als Watson van IBM zorgen nu al voor snellere en betere (kanker)diagnoses. Robots als Da Vinci en de Japanse zeehond Paro kunnen chirurgen, verpleegkundigen en (mantel)zorgverleners ontlasten bij het opereren, verzorgen en aandacht geven. Met 3D-printers (bioprinters) kunnen we allerlei organen maken, met gentherapie kunnen we auto-immuunziekten behandelen, bionische ledematen kunnen beschadigde lichaamsdelen vervangen en met geïmplanteerde chips kunnen we ons lichaam voortdurend monitoren of bepaalde hersenziekten en stoornissen verhelpen.

Dat dit een ongemakkelijk gevoel geeft is begrijpelijk maar een simpele robot die helpt medicijnen op tijd in te nemen, kost geen werkgelegenheid en voorkomt hogere zorgkosten. Robots komen zo naast mensen te staan. D66 wil dat Nederland veel meer gebruik maakt van digitale zorgmogelijkheden en beter samenwerkt om dit te realiseren in ziekenhuizen en zorginstellingen.

D66 stelt voor:

- Zet zorgrobots op grote schaal in maar doe dit geleidelijk. Laat de geboekte tijdwinst daarbij ten goede komen aan persoonlijk contact met de patiënt en het bestrijden van eenzaamheid bij ouderen.
- Waarborg dat menselijk contact onlosmakelijk onderdeel van de zorg blijft. Robots nemen geen zorgbanen over, maar zorgtaken. Maak het voor mensen mogelijk om zich te concentreren op zorgtaken die robots niet over kunnen nemen.
- Laat zorginstellingen, die erin slagen om door de inzet van nieuwe technologie lagere zorgkosten te bewerkstelligen, deze besparing twee jaar houden om in te zetten voor onderzoek en innovatie die de zorgkwaliteit verbetert.
- Verzamel digitale patiëntinformatie via patiëntendossiers om de zorg te verbeteren. Maar doe dit alleen onder de voorwaarde van stevige privacy-waarborgen, op het gebied van data-eigendom en (medische) doelbinding.

- **Verspreid alle beschikbare medische kennis zo goed mogelijk digitaal met het oog op de grote gezondheidswinst die dit oplevert. Minimale kwaliteitseisen en voldoende actuele kennis bij de behandelend arts zijn cruciale factoren.**

Kader 4: met een eenvoudig apparaatje en een beveiligde verbinding kan de huisarts op afstand een hartfilmpje door een cardioloog laten uitlezen. Met een paar handelingen in een app kan de cardioloog het filmpje beoordelen en zo nodig overleggen met de huisarts. Voor eenvoudige behandeling wordt de patiënt zo een tijdrovende en kostbare ziekenhuisafspraak bespaard. Meer van deze behandelingen zouden bij de huisarts uitgevoerd kunnen worden.

Dit is slechts een van de vele voorbeelden waarbij zorg op afstand kan worden geleverd. Zo zou er ook door een dermatoloog op basis van een toegestuurde foto een diagnose gesteld kunnen worden of zou een huisarts een online consult kunnen doen. Belangrijke voorwaarden zijn een betrouwbare internetverbinding maar vooral apparaten en apps met veilige hard- en software. Aan de leveranciers van zulke zorgproducten moeten dus eisen gesteld worden.

Digitale overheid

Bijna iedereen doet zijn belastingaangifte naar tevredenheid online. Toch is lang niet iedereen gelukkig met de digitale overheid. Sommigen zien digitaal contact met de overheid als makkelijker, anderen zien een overheid die moeilijker bereikbaar is, bureaucratie die zorgt voor vervreemding en efficiency in plaats van de menselijke maat. Door wildgroei aan overheidswebsites, zijn veel bomen in het bos bijvoorbeeld niet meer zichtbaar. De één-digitaal-loket-gedachte is daarom aanlokkelijk maar de keerzijde is dat koppeling van bestanden en centralisatie persoonsgegevens kwetsbaarder maken voor diefstal. Dit dilemma vraagt om een evenwichtige inrichting van de digitale overheid.

Een ander knellend vraagstuk vormen de onhaalbare en onbeheersbare ICT-projecten die ver uit de tijd en de kosten lopen. Dit omdat verkeerde prikkels mislukkingen in de hand werken, er een angstcultuur is ontstaan, de projectvoering rigide is en de sturing niet gepaard gaat met goed risicomanagement. De controle op ICT-projecten is niet onafhankelijk en de overheid leunt nog steeds teveel op een beperkt aantal aanbieders. Daarbij verzwakt de manier van aanbesteden de grip op ICT-projecten, die veel te groot worden opgezet. Mislukkingen worden zelden toegegeven waardoor er onvoldoende van geleerd wordt. Ook wordt er nog te veel met gesloten standaarden gewerkt waardoor de overheid zelf min of meer gedwongen is om software van één ICT-leverancier te blijven kopen, omdat alleen zo de informatie gebruikt kan blijven worden.

Het databeheer is evenmin op orde. Zo is privacy niet gewaarborgd en is de Europese privacywet Algemene Verordening Gegevensbescherming (AVG) nog geen werkelijkheid. Daarnaast moeten mensen meer regie krijgen over hun eigen persoonsgegevens. Inzien wie jouw gegevens gebruikt is nu erg ingewikkeld, en de Basisregistratie Personen wijzigen levert een bureaucratisch doolhof op. Verder bezit de overheid veel publieke data en wordt onderzoek gedaan van publiek geld zonder dat het gratis beschikbaar is. Ook is veel overheidssoftware niet standaard openbaar en worden niet altijd open standaarden gebruikt, terwijl die wel veiliger zijn.

Tot slot gebruikt de overheid steeds meer algoritmes bij besluitvorming. Dit kan verkeerd uitpakken. De burger mag geen slachtoffer zijn van een robotachtig speelveld, waarin een menselijk oog voor de precieze situatie verdwijnt[17]. Dit vraagt om uitlegbaarheid en controleerbaarheid, waar we in het volgende hoofdstuk op ingaan.

Ook in de digitale wereld moet de overheid te alle tijde voldoen aan algemene beginselen van behoorlijk bestuur. Om de digitale overheid in goede banen te leiden, zijn duidelijke uitgangspunten nodig, zoals toegankelijkheid; transparantie; uitlegbaarheid; gegevensbescherming; deskundigheid en lenigheid.

D66 stelt voor:

- **Stel de mens centraal via verschillende opties. De één krijgt een pushbericht, de ander een papieren verzoek. Bied de groep digitaal laaggeletterden de nodige aandacht en hulp: investeer in de digitale weerbaarheid van iedereen.**
- **Streef naar een papierarme manier van communiceren in 2030. Geef ouderen, mensen met een migratieachtergrond, minima, en verstandelijk beperkten actief hulp of desnoods een niet-digitaal alternatief.[18]**
- **Maak via mijnoverheid.nl beter inzichtelijk door wie, wanneer en waarom informatie uit de Basisregistratie Personen (BRP) of het patiëntendossier is opgevraagd.**
- **Communiceer als overheid attent en veilig met burgers. Bijvoorbeeld door de berichtenbox-app en zonder gebruik te maken van Whatsapp of Facebook.**
- **Geef iedereen een persoonlijke digitale kluis voor zijn persoonsgegevens en haal als overheid gegevens hieruit volgens de één-bron gedachte. Het voorkomt dubbele opslag en maakt inzage en correctie makkelijker[19].**

[17] Hierover schrijft ook de Raad van State in haar recente ongevraagd advies over de digitaliserende overheid: https://www.raadvanstate.nl/pers/persberichten/tekst-persbericht.html?id=1178

[18] Hiervoor zou kunnen gekeken worden naar de campagne 'Da's toch handig, dat internet!' die door de Vlaamse Overheid is opgezet: https://cjsm.be/media/themas/mediawijsheid/campagne-das-toch-handig-dat-internet.

[19] Zie hiervoor de initiatiefnota van Middendorp en Verhoeven: https://zoek.officielebekendmakingen.nl/kst-34993-2-n1.html

- Maak het Nederlandse 'E-Burgerschap' mogelijk: een digitale service waarbij je een E-ID kaart krijgt waarmee je onder andere een bedrijf kan opzetten in het land, zonder daadwerkelijk in het land te wonen of te werken.[20]
- Maak publieke data, met inachtneming van privacy risico's, waar mogelijk openbaar. Publieke software is zoveel mogelijk open source en wordt ook weer gedeeld. Geef bij inkoop voorkeur aan open source software. Zo niet, leg dan uit waarom niet.
- Knip megaprojecten op in kleinere gedeelten en werk met een "minimum viable product". Zo blijven projecten behapbaar en wordt de afhankelijkheid van leveranciers verminderd. Kies waar nodig voor 'insourcing', bijvoorbeeld de controle op algoritmes of infrastructuur voor digitale identificatie.
- Start een Rijksingenieursbureau, vergelijkbaar met dat van de Britse overheid. Behalve een orgaan dat ongevraagd kan adviseren, creëren we zo een groep Rijksspecialisten (programmeurs) die door de overheid heen inzetbaar zijn.
- Wees als overheid terughoudend met het delen en koppelen van data. Waar persoonsgegevens verzameld worden is privacybescherming en informatieveiligheid vanaf het begin onderdeel van het ontwikkelingsproces.
- Maak bij elk besluit waarbij een algoritme is gebruikt, de dataset herleidbaar en garandeer dat beslisregel plus onderbouwing hiervan toetsbaar zijn. Maak "menselijke" heroverweging wanneer iemand bezwaar maakt, altijd mogelijk.

Kader 5: Estland loopt voorop in Europa als het gaat om de digitale overheid. Als een ambtenaar naar de gegevens kijkt, dan krijgt de burger daar een melding van. Elke actie laat een digitaal spoor achter. Hierdoor is iedereen altijd op de hoogte wat er met zijn of haar data gedaan wordt en wie hier inzage in heeft. Overtredingen kunnen via de melding worden gesignaleerd en indien van toepassing ook gecorrigeerd. In de fysieke wereld is dat niet altijd vanzelfsprekend, aangezien juist veel moeilijker gecontroleerd kan worden wie er in persoonlijke gegevens kijkt.[21]

[20] NOS: https://nos.nl/nieuwsuur/artikel/2188442-een-volledig-digitale-samenleving-in-estland-kan-het.html
[21] NRC: "De EU mag wel wat harder rennen, vindt e-Estonia. URL: https://www.nrc.nl/nieuws/2017/10/02/de-eu-mag-wel-wat-harder-rennen-vindt-e-estonia-13293644-a1575670).

Hoofdstuk 2. Kunstmatige Intelligentie: investeren, reguleren, herverdelen

De afgelopen decennia hebben verschillende technologieën voor maatschappelijke veranderingen gezorgd. Het internet en mobiele telefoons ontsloten de wereld, het internet der dingen verbond miljarden apparaten en 3D-printen maakte persoonlijke productie mogelijk. Van andere technologieën is nog niet duidelijk wat hun impact zal worden, zoals bij blockchain en quantumcomputing. Sommige zullen overschat worden, andere juist onderschat.

Een ding is duidelijk. De meest ingrijpende technologie van dit moment is kunstmatige intelligentie. Er zijn vele definities voorhanden[22] maar kort samengevat is kunstmatige intelligentie (KI) de wetenschap die zich bezighoudt met het creëren van systemen met een vorm van intelligentie. Het is het deel van de informatica dat zich richt op systemen die functies uitvoeren die we normaal gesproken associëren met het menselijk brein[23]. Kunstmatige intelligentie is een concept waarbij apparaten reageren op data of impulsen en op basis daarvan zelfstandige beslissingen nemen[24].

Kader 6: KI is niet nieuw. In 1950 stelde wiskundige en computerpionier Alan Turing de vraag of machines zouden kunnen denken en hij ontwikkelde een test voor machine intelligentie, de zogenaamde Turing test[25]. Kort daarop, in 1952, ontwikkelde Arthur Samuel een machine die mensen kon leren dammen. In 1956 muntte computerwetenschapper John McCarthy de term "kunstmatige intelligentie". Het werd voor het eerst concreet op 10 februari 1996, toen versloeg de computer Deep Blue van IBM de regerende wereldkampioen schaken Gary Kasparov. Tot die tijd werd schaken beschouwd als het belangrijkste voorbeeld van menselijke superioriteit. Dit succes markeerde het hoogtepunt van de eerste generatie KI-systemen, gebaseerd op kennistechnologie met expliciet geformuleerde regels (algoritmes).

Een nieuwe doorbraak kwam in 2006 toen Geoff Hinton en Ruslan Salakhutdinov een artikel publiceerden met de titel "Reducing the dimensionality of data with neural networks". De stap naar zogenaamde diepe neurale netwerken maakte de stap van menselijke input naar "machine learning" mogelijk. Hierbij leert de computer zelf en zijn geen vooraf geformuleerde regels nodig. Dit vergrootte de potentie van KI naar complexere toepassingen. Dit bleek toen de IBM-computer Watson twee

[22] De definitie van Google in "Making AI" luidt: "Artificial Intelligence is the science of making machines that appear intelligent". Luka Crnkovic-Friis schrijft in "The Essential AI Handbook for Leaders (2018): "Artificial Intelligence is a set of computer sciences that allows computer software to learn from experience, adapt new inputs and complete tasks that resemble human intelligence".
[23] Deze uitleg is afkomstig uit "AI voor Nederland" van AINED, een samenwerkingsverband tussen bedrijfsleven en wetenschap.
[24] Deze uitleg is afkomstig uit "Het verhaal van digitaal" van ECP, Platform voor de InformatieSamenleving.
[25] Als een machine vragen zodanig kan beantwoorden dat hij mensen kan overtuigen dat hij een mens is, is de machine intelligent.

mensen versloeg in het spel Jeopardy!, een computerprogramma van Google (Deepmind) zichzelf Atari-games leerde spelen en de computer AlphaGo de regerend wereldkampioen Go versloeg. De subtiele complexiteit van Go werd onbereikbaar geacht voor een computer maar deze trok zich daar weinig van aan.

De impact van Kunstmatige Intelligentie

Er is een aantal redenen waarom KI de technologie is met de grootste impact. Allereerst is KI centraal onderdeel van alle belangrijke vormen van digitalisering en kan het alle domeinen en sectoren beslaan. KI is dus een generieke technologie. Ten tweede is er nu een bloeiperiode door de cruciale stap naar machine learning. Deze wordt aangejaagd door de enorme stijging van de hoeveelheid data, onder meer door cloudopslag en de explosie van het internet dingen, waarbij jaarlijks miljarden apparaten op het internet worden aangesloten, en de steeds grotere rekenkracht van (super)computers.

Niet voor niets wordt kunstmatige intelligentie al op vele terreinen toegepast. En dit gaat veel verder dan mensen vaak doorhebben. Denk aan navigatieapps, beeldherkenning, het ogenblikkelijk kunnen vertalen van teksten, spamfilters en zelf parkerende auto's. En uiteraard gebruiken bedrijven als Google, Facebook, Alibaba, Amazon, Spotify, Netflix, Airbnb en Uber algoritmes om de consument te sturen naar de volgende link, like, aankoop, playlist, serie, hotel of taxirit. Waarmee ze overigens hun macht steeds verder vergroten (zie hoofdstuk 3).

Niet te vergeten, ook overheden gebruiken steeds vaker algoritmes. Zo heeft het ministerie van Binnenlandse Zaken een proef voor de analyse van kindermishandeling en migratie met KI. En ook in de fraudebestrijding, belastingplicht en verkeersbegeleiding worden algoritmes ingezet. Zoals bij alle technologie zijn er duidelijke kansen maar evenzeer serieuze bedreigingen. De lastige maar noodzakelijke opgave is om hier een goed evenwicht te vinden. De politiek heeft hier een cruciale rol maar kan die alleen invullen als er voldoende kennis van zaken is, een voorwaarde waaraan nu nog niet is voldaan.

Kader 7: KI kan in theorie heel ver strekken. In zijn duizelingwekkende boek LIFE 3.0[26] laat Max Tegmark, professor natuurkunde aan MIT, zien waarom. Hij beschrijft intelligentie als het vermogen om complexe doelstellingen te bereiken en benadrukt het verschil tussen beperkte intelligentie (zoals Deep Blue) en algemene intelligentie (zoals de mens). KI kan veel, maar ook heel veel nog niet. Momenteel wint menselijke intelligentie het ruimschots qua algemeenheid van kunstmatige intelligentie maar zijn machines ons de baas in steeds meer specifieke taken.
De vraag is of dit altijd zo blijft want de KI-wetenschap wil een zo hoog mogelijk algemene kunstmatige intelligentie (AKI)

[26] Max Tegmark: Life 3.0 (2017). Het hele boek is geweldig maar de hoofdstukken 2 en 6 gaan in op natuurwetten en leervermogen. Een *must read* voor iedereen die niet gelooft dat machines de mens steeds dichter naderen.

realiseren, uiteindelijk zelfs superintelligente KI. Het moment dat machines de menselijke intelligentie in alle opzichten overtreffen, is door futurist Ray Kurzweil gedoopt als technologische singulariteit. Het is nu nog puur theoretisch maar wetenschappelijk uitgesloten is het op basis van natuurwetten zeker niet. In dit kader wijst Yuval Harari op de grote ontkoppeling tussen intelligentie en bewustzijn: het bewustzijn van computers staat nog niet eens in de kinderschoenen en de wetenschap boekt hier weinig vooruitgang. Maar dat maakt niet uit want intelligentie is voor veel taken relevanter dan bewustzijn[27].

Dat het mogelijk is menselijke intelligentie te overtreffen laat Tegmark zien via de werking van ons geheugen, computatie en leervermogen. Hij maakt duidelijk dat elk materiaal als substraat kan dienen voor het geheugen, mits het verschillende stabiele toestanden kent. Daarbij kan alle materie -onder voorwaarden- dienen als computronium. Computronium is een uitvoerder van willekeurige berekeningen. NAND-poorten en neuronen zijn de bekendste voorbeelden. Daarbij legt hij uit hoe een neuraal netwerk in staat is zelf zijn structuur aan te passen om beter te worden in de functie waar hij voor gemaakt is. Oftewel: zelflerendheid (deep learning).

Drie KI-uitdagingen: achterstand, rechtenschending en tweedeling

Om als politiek evenwichtig met het onderwerp KI om te gaan is het nodig het voldoende in te kaderen. Zolang de wetenschap nog niet heeft kunnen bewijzen hoe en wanneer een machine de mensen op alle fronten de baas is, hoeven we daar politiek geen rekening mee te houden. Ook moeten we alle doemscenario's van intelligente machines die de mens overheersen en uitroeien relativeren, al is de onzekerheid die dit met zich meeneemt wel een factor van betekenis[28]. Enige basiskennis van de technische werking van verschillende varianten van machine learning (zoals deep learning, reinforcement learning, supervised learning en unsupervised learning) is voldoende.

De praktijk moet centraal staan bij de politieke aanpak van KI. Namelijk dat kunstmatige intelligentie -van simpele rekenformules tot zelflerende systemen- wordt ingezet om problemen op te lossen en dat dit grote voordelen kan hebben op het gebied van onderwijs, zorg, verkeersveiligheid en milieubescherming: KI kan specifieke leerbehoeftes in kaart brengen, kanker sneller herkennen, zelfrijdende auto's besturen en cyber-aanvallen detecteren.

[27] Harari: Homo Deus (205), p. 321 en verder.
[28] Hoewel: Mensen als Elon Musk en Stephen Hawkins hebben erop gewezen dat zelfs een KI-systeem met een goede intenties of een onschuldige functie uiteindelijk (onverwachte) zelfstandige beslissingen kan nemen om zijn doel te bereiken ten koste van de mensheid of zijn doel aan te passen ten koste van de mensheid. De zelflerendheid die nu tot de mogelijkheden behoort, sluit dit inderdaad niet uit.

Naast veel potentie brengt KI een drietal serieuze uitdagingen met zich mee. Allereerst, het meest urgent, een internationale concurrentieslag. Aan weerszijden van ons continent strijden China en de VS om de positie van KI-wereldleider. Europa dreigt hierbij –qua wetenschappelijk onderzoek, bedrijfsinvesteringen, hoeveelheid patenten- achterop te raken, wat uiteindelijk onze concurrentiekracht en welvaart bedreigt. Dit vraagt om extra investeringen. Ten tweede is duidelijk geworden dat KI-toepassingen grondrechten, burgerrechten en maatschappelijke waarden onder druk kunnen zetten. Dit moet op korte termijn worden opgevangen door regulering op basis van ethische principes. Ten derde, op langere termijn, is er het scenario van verlies van werkgelegenheid, dat kan leiden tot toenemende onzekerheid, afnemende betrokkenheid en diepere maatschappelijke tweedeling. Dit vraagt om verschillende vormen van herverdeling.

Deze drie uitdagingen leiden tot een gepolariseerd debat[29]. Enerzijds heb je de techno-optimisten die vrezen dat het doemdenken en de bangmakerij van sommige critici en politici leidt tot stilstand en dus achterstand en achteruitgang. Ook vrezen zij dat de ethische discussie en regulering investeringen in de weg staat. Anderzijds heb je de techno-pessimisten die vrezen dat het blinde geloof in technologie de maatschappij (onomkeerbaar) zal ontwrichten. Ze vrezen dat er onvoldoende oog is voor ongewenste gevolgen, omdat er alleen maar gekeken wordt naar technische mogelijkheden en economische verhoudingen. Niet naar de consequenties voor mensen. Beide kampen hebben recht van spreken en juist daarom is een genuanceerde en gebalanceerde discussie over kansen en bedreigingen cruciaal. D66 kiest voor een middenweg met zowel investeren in KI om de mens te laten profiteren als reguleren en herverdelen om de mens te beschermen.

Kader 8: Dat KI talloze toepassingen kent, is duidelijk. Maar wat zijn nu de grootste kansen en bedreigingen van KI? Europese wetenschappers[30] en beleidsmakers[31] denken hier al langer over na. De vier belangrijkste mogelijkheden zijn:
Individuele ontplooiing en zelfrealisatie (door tijdbesparing en specialisatie);
Beter menselijk handelen (door snellere besluitvorming);
Maatschappelijke mogelijkheden vergroten (door slimmere systemen);
Meer coördinatie en samenwerking (door meer grip op complexiteit).

De eerste bedreiging is het niet benutten of onderbenutten van de kansen, bijvoorbeeld door angst of een gebrek aan prioriteit, geld of kennis. Daarnaast zijn er vier bedreigingen van overmatige en ongecontroleerde inzet van KI:
Afwaardering van menselijk vermogen ("deskilling");

[29] In de Groene Amsterdammer van 17 mei 2018 schreef Luciano Floridi hier een lezenswaardig artikel over: "Over Singularitarianen en AItheisten"
[30] AI4People: "An Ethical framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations" (December 2018), te verschijnen in *Minds and Machines*.
[31] The European Commission's High-Level Expert Group on AI: "Ethic Guidelines for Trustworthy AI" (December 2018)

Wegnemen van menselijke verantwoordelijkheid ("The computer says no");
Verminderen van menselijke controle ("overruling");
Uitholling van menselijke zelfbeschikking ("undermining human dignity").

Bekende praktijkvoorbeelden zijn zelfrijdende auto's die betrokken raken bij een ongeluk of autonome wapens (killer robots) in een oorlog (wie is aansprakelijk?), de ongrijpbaarheid van KI-besluitvorming (hoe komt een besluit precies tot stand?) of algoritmes die bepaalde groepen discrimineren of buitensluiten ('biased' black boxes).

Opleiden, stimuleren en investeren

Zoals beschreven heeft KI veel goeds gebracht, maar het kan nog veel meer goeds brengen. Het is zaak deze mogelijkheden optimaal te benutten door te investeren in wetenschappelijk onderzoek en praktische toepassingen. De grote internationale concurrentie maakt dat we daar niet te lang mee moeten wachten. Nederlandse wetenschappers en het verenigde bedrijfsleven, verenigd in samenwerkingsverband AINED, wijzen in dit verband op de sneltreinvaart waarmee andere landen KI omarmen. Zo wil China in 2030 wereldleider zijn, investeren Amerikaanse bedrijven vele miljarden in algoritmes, heeft Frankrijk onder leiding van Macron een AI-strategie, noemt Merkel het een nationale topprioriteit en heeft het Verenigd Koninkrijk een AI Sector Deal en geld voor 1.000 AI-promovendi[32].

Uit onderzoek van Elsevier blijkt intussen dat het aantal wetenschappelijke citaten van Europese onderzoekers daalt ten faveure van Chinese en Amerikaanse concurrenten[33]. Naast politieke urgentie en publiek geld ontbreekt het echter aan voldoende onderwijscapaciteit om in KI geïnteresseerde studenten op te nemen. Daarnaast wordt op teveel middelbare scholen geen goed informatica-onderwijs gegeven wegens een tekort aan geschikte leerkrachten. Op wetenschappelijk onderzoeksgebied is weliswaar nog geen sprake van het massaal wegtrekken van Nederlands talent, maar een dergelijke braindrain dreigt wel, want er wordt wereldwijd aan onze KI-talenten getrokken door buitenlandse universiteiten of door grote techbedrijven.

Genoeg reden voor politieke actie maar in de Tweede Kamer is het oorverdovend stil. Een D66-voorstel om 25 miljoen euro te investeren in KI werd recentelijk verworpen door de Tweede Kamer. Het gevoel van urgentie ontbreekt en als het al over KI gaat, dan ligt de nadruk op de mogelijke negatieve gevolgen. Volgens de onafhankelijke denktank Denkwerk is het politieke debat de verkeerde kant op geschoven. We missen daardoor de

[32] AINED (Topteam ICT, VNO-NCW, ICAI, NWO, TNO, BCG en DenkWerk): "AI voor Nederland, Vergoten, versnellen en verbinden" (2018)
[33] Elsevier: "Artificial Intelligence: How knowledge is created, transferred, and used" (2018)

kans om positieve impact met KI te realiseren en we delven het onderspit in de omvang van investeringen[34]. Ze roepen op tot politieke daadkracht in de vorm van een Nationale KI-agenda. Nederland moet op basis hiervan samen met bedrijfsleven en universiteiten het stuur pakken. De denktank Denkwerk wijst er terecht op dat een koploperspositie noodzakelijk is om zowel je eigen koers te kunnen bepalen als de ethische grenzen van KI in groter verband te bewaken. Oftewel: zonder investeringen is de droom van een Europese rol als ethisch leider in KI een illusie.

De KI-potentie van Nederland is nog steeds groot maar als gevolg van investeringsangst bij bedrijven, een kennisachterstand bij de overheid en een risicomijdende houding is Nederland langzaam aan het afglijden ten opzichte van landen als Canada, Israël en Singapore. Wel moet benoemd worden dat de Europese cultuur ten opzichte van privacy en data, de kritische brandstof van KI, hierin een rol speelt[35]. Maar ook met behoud van burgerrechten en oog voor ethiek is het mogelijk om meer te investeren en beter te innoveren dan nu het geval.

D66 stelt voor:

- Verbeter de KI-kennis en organisatie binnen de overheid structureel. Een hoge Digitale Autoriteit (of een ministerie van Digitale Zaken) helpt hierbij (zie hoofdstuk 5).
- Verhoog de capaciteit van het KI-onderwijs, zodat meer studenten opgeleid kunnen worden. Een goed streven is 1.000 studenten per jaar.
- Verhoog het onderzoeksbudget voor KI fors. Kijkende naar vergelijkbare en ons omringende landen is op termijn een half miljard euro per jaar nodig. Wetenschap en bedrijfsleven hebben in dit kader gepleit voor een (revolverend) KI-groeifonds binnen het nationale investeringsfonds Invest-NL.
- Benut bestaande innovatie-instrumenten als de SBIR-regeling, de PPS-toeslag en de MIT-regeling beter. Laat publieke onderzoeksinstellingen als TNO een substantieel groter deel van hun budget aan KI besteden.
- Investeer extra in wetenschappelijk onderzoek naar *explainable artificial intelligence* (X.A.I): KI-systemen die hun eigen keuzes kunnen uitleggen waardoor gemaakte beslissingen beter controleerbaar zijn. Hier ligt een mooie kans voor Nederland.

[34] DenkWerk: Artificial Intelligence in Nederland (2018)
[35] Grofweg zou je kunnen zeggen dat data in China staatseigendom zijn, in de Verenigde Staten handelswaar (bedrijfseigendom) en in de Europese Unie een individueel recht (eigendom van burgers).

- Moderniseer regelgeving. Het beter verspreiden van publieke data en afdwingen van data-delen kan alleen met volledige naleving van geldende privacy-eisen.

Rechten, waarden en principes

Tot nu toe heeft de discussie over ethiek en technologie zich hoofdzakelijk beperkt tot privacy. Bedrijven verzamelen persoonsgegevens van consumenten voor een commercieel doeleinde, overheden verzamelen persoonsgegevens van burgers voor een controle-doel. Hier zijn we in de Techvisie 1.0 uitgebreid op in gegaan. Inmiddels zijn er met de uitbreiding van de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt, de aanpassing van de wet op de inlichtingen- en veiligheidsdiensten (wiv), en de inwerkingtreding van de Europese Privacywet (AVG) stappen gezet. Uiteraard zorgt de combinatie van KI, big data, cloudtechnologie en het internet der dingen voor nieuwe uitdagingen. Het blijven ontwikkelen van wetgeving, zoals de ePrivacy-verordening van de Europese Unie blijft daarom nodig.

Door de komst van algoritmes is het tijd de discussie te verbreden van privacy naar het bredere domein van grondrechten, burgerrechten en maatschappelijke waarden. Want dat algoritmes meer kunnen treffen dan privacy is inmiddels wel duidelijk. Volgens de WRR heeft KI een toenemende invloed op ons dagelijks leven[36]. Volgens het Rathenau Instituut komen gelijke behandeling, autonomie en waardigheid onder druk te staan[37]. De Raad van State waarschuwde onlangs dat de burger niet in de knel mag komen door de digitaliserende overheid en dat digitale besluiten beter gemotiveerd moeten worden. En de Commissie Remkes wees op het risico van minder transparantie en aangetaste autonomie als gevolg van algoritmes die politieke informatie rangschikken[38].

Een uitgebreide studie van de Universiteit Utrecht zet de grondrechtelijke knelpunten van algoritmes op een rij en wijst daarbij op mogelijke schendingen van privacyrechten (datasurveillance, 'chilling effect', relationele privacy en het recht vergeten te worden), gelijkheidsrechten ('discriminatie door biases', schijnneutraliteit), vrijheidsrechten (filterbubbels, censuur, demonstratierecht, selectieve toelating) en procedurele rechten (rechtstoegang en onpartijdigheid)[39].

Niet alles zal zich even snel voltrekken maar waakzaamheid is geboden. Belangrijk inzicht hierbij is het feit dat technologie niet per se neutraal is en een computer niet per se objectief en rechtvaardig. Tijdens een hoorzitting in de Tweede Kamer zei Virginia Eubanks, de Amerikaanse auteur van "Automating Inequality", dat "algoritmes geen

[36] Zie: https://www.wrr.nl/publicaties/rapporten/2011/03/15/ioverheid
[37] Zie: https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen
[38] Staatscommissie Parlementair Stelsel: "Lage Drempels, Hoge Dijken" (2018)
[39] Vetzo, Gerards & Nehmelman: "Algoritmes en Grondrechten" (Universiteit Utrecht, 2018)

administratieve tools zijn maar systemen voor politieke besluitvorming"[40]. Om het in de toekomst menselijk te houden, moet KI daarom verbonden worden aan sociale, ethische en juridische waarden en wetten. Dat zag ook de eerder aangehaalde KI-wetenschapper Max Tegmark. Hij is tevens oprichter van het "Future of Life Institute (FLI)[41], dat in januari 2017 een grote bijeenkomst organiseerde waar vele relevante deskundigen in KI (en aanverwante gebieden) bijeen kwamen. Deze bijeenkomst in Asilomar leidde tot de zogenaamde KI-principes van Asilomar: 23 principes die moeten leiden tot een positieve ontwikkeling van KI[42].

Deze principes zijn onderverdeeld in drie categorieën. Allereerst onderwijskwesties die stellen dat het onderzoeksdoel goedaardige KI moet zijn en dat de financiering, cultuur en samenwerking hierop gericht moeten zijn. Ten tweede moeten morele waarden centraal staan zoals veiligheid, transparantie, toezicht, verantwoordelijkheid, menselijkheid, vrijheid en privacy, gedeeld voordeel en geen KI-wapenwedloop. Ten derde moeten lange termijnkwesties behandeld worden die vooral gaan over het moment dat er algemene KI is en het waarborgen van het algemeen welzijn. Vele instanties, overheden en bedrijven (zoals Google en Microsoft) hebben vergelijkbare principes geformuleerd. De politieke uitdaging waar we nu voor staan is om de abstracte KI-principes te vertalen naar concretere KI-eisen en KI-acties. Dat is niet eenvoudig.

Kader 9: De bedreigingen van KI vragen om een kader gebaseerd op fundamentele rechten, maatschappelijke waarden en ethische principes. De al eerder genoemde KI-wetenschapers van AI4People hebben een framework gemaakt op basis van het werk van verschillende organisaties (waaronder de Asilomar AI Principles). Dit kader is gebaseerd op kernprincipes uit de bio-ethiek en vormt inmiddels ook uitgangspunt voor de Europese Commissie. Deze vijf principes zijn:

1. Weldadigheid. Goed voor de menselijke waardigheid en behoud van de planeet;
2. Onschadelijkheid. Behoud van privacy en veiligheid. Voorzichtige inzet.
3. Autonomie. De mogelijkheid om te beslissen (waarover je beslist)
4. Rechtvaardigheid. Vergroot de welvaart en behoud de solidariteit.
5. Verklaarbaarheid. Uitleg geven. Het begrijpelijk maken. Verantwoording afleggen.

Deze abstracte principes kunnen concreet gemaakt worden door ze te vertalen naar praktische eisen, zoals de High-Level Expert Group van de Europese Commissie doet. Zij komen tot tien eisen: aanspreekbaarheid en compensatie; data-regulering; algemeen toegankelijk; menselijke controle; non-discriminatie; diversiteit en pluriformiteit; privacybestendig; betrouwbaar en weerbaar; veilig en transparant. Op basis van deze vereisten kunnen (technische en organisatorische) acties worden

[40] Ook de Amerikaanse wiskundige Cathy O'Neil heeft in haar boek "Weapons of Math Destruction" (2016) gewezen op het gevaar dat algoritmes en big data de economie ontwrichten en de democratie ondermijnen.
[41] Zie: https://futureoflife.org
[42] Zie voor de 23 principes en onderteken ze als je wilt: https://futureoflife.org/ai-principles/

ondernomen.

In Nederland is het nog relatief stil op dit gebied. Die stilte moet doorbroken worden want juist door duidelijke grenzen en kaders te bieden, is het mogelijk om meer vaart en de juiste richting aan KI te geven.

D66 stelt voor:

- Formuleer als kabinet Nederlandse KI-principes die het gebruik van KI in algemene zin de gewenste richting en de nodige begrenzing geven. De Digitale Top in maart 2019 is hiervoor het juiste moment.
- Formuleer op basis hiervan concrete KI-eisen waaraan voldaan moet worden bij de inzet van algoritmes, zowel door overheden als bedrijven in Nederland. Sluit hierbij nauw aan bij de vijf principes en tien vereisten zoals geformuleerd door AI4People en de Europese Commissie (zie kader). Op basis hiervan zijn technische, organisatorische en wetgevende acties mogelijk.
- Stel grenzen aan besluitvorming door KI. Als de maatschappelijke nadelen de voordelen overstijgen, wordt de inzet van KI stopgezet. Toets of bestaande instituties, wetten en regels voldoende zijn toegerust op KI.
- Zorg voor een humane inzet van algoritmes. Te beginnen met "*ethics by design*". Dwing daarnaast transparantie, toetsbaarheid, inzichtelijkheid en uitlegbaarheid[43] af. Zorg voor audit-systemen[44] en de mogelijkheid tot correctie en compensatie.
- Organiseer brede betrokkenheid. Dus geen KI-debat tussen technici en informatici maar een brede maatschappelijke discussie met sociale en juridische invalshoeken, samenwerking tussen verschillende disciplines, verantwoordelijke bedrijven en goed geïnformeerde burgers. Keurmerken, gedragscodes, ethische commissies, standaardcontracten en campagnes maken hier onderdeel van uit.
- Stel een algoritme-waakhond in, die toezicht houdt op de inzet van algoritmes (en onderliggende datasets) door overheid en bedrijven met grote maatschappelijke impact en die de gevolgen voor mensen toetst en waar nodig corrigeert. Toets algoritmes tevens aan de grondwet.
- Geef KI-studenten niet alleen informatica maar leer ze ook kernaspecten van de filosofie, sociologie, psychologie, en mensenrechten.

[43] Verschillende deskundigen wijzen erop dat uitlegbaarheid bij machine learning tegen grenzen aanloopt omdat dan niet duidelijk is waarom een systeem tot een bepaald besluit is gekomen. In dat geval moet dit meegewogen worden in de inzetbaarheid van het algoritme.

[44] New York heeft een werkgroep ingesteld die gaat controleren of algoritmes die voor ambtelijke besluitvorming worden ingezet niet discrimineren: https://www.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html

Werkgelegenheid en tweedeling

Dit hoofdstuk eindigt met een thema dat zeker in de huidige economische groei nog geen concrete vorm aanneemt, maar wat op langere termijn wel degelijk grote gevolgen kan hebben: de invloed van KI op de menselijke werkgelegenheid en een menselijke samenleving. Dat nieuwe technologieën invloed hebben op banen, beroepen en werkgelegenheid, hebben eerdere industriële revoluties stuk voor stuk uitgewezen. We kennen allemaal het verhaal van de Luddieten die in opstand kwamen tegen de weefmachines. Nu kwamen er tijdens deze revoluties uiteindelijk meer nieuwe (en betere!) banen bij en groeide de welvaart, dus is een vaak gehoorde inschatting dat ook tijdens de huidige vierde industriële revolutie[45] het vooral zal gaan om een positieve verschuiving in plaats van een totaal verlies.

Deze voorspelling lijkt uit te komen waar het gaat om de gevolgen die de Nederlandse arbeidsmarkt ondervindt door de inzet van robots. Deze discussie laaide een aantal jaar geleden op en de vrees van vakbonden en politici dat robots tot werkeloosheid zouden leiden is vooralsnog geen werkelijkheid geworden. De OESO publiceerde in 2018 een onderzoek waaruit bleek dat het verdwijnen van banen door robots beperkt is en dat de Nederlandse baan tamelijk robotproof is: slechts 11,4% van onze banen loopt grote kans geautomatiseerd te worden. Voor sommige EU-landen ligt dat overigens tegen de 30%[46].

Toch moet daarbij een aantal kanttekeningen gemaakt worden. Allereerst ligt het aantal banen dat zodanig verandert dat nieuwe vaardigheden nodig zijn, veel hoger, namelijk op 28% (OESO). Daarbij leidt de verandering van werk ook tot een arbeidsmarkt waarbij het midden onder druk staat (baanpolarisatie) en de kwaliteit van werk afneemt. Verder strekken de mogelijkheden van machine learning veel verder dan de generatie robots die zijn werk doet op de landbouwgrond, in de fabriekshal en aan het bureau. De computers van de 21e eeuw zijn steeds geavanceerder en hebben toepassingen die meer vervangen dan fysieke en administratieve arbeid alleen. Bovendien voeren ze hun werk zelfstandiger uit. Dit betekent dat op termijn haast geen enkel beroep niet door een computer kan worden uitgevoerd[47].

Tegelijkertijd is het geruchtmakende onderzoek “The Future of Employment” van Frey en Osborne uit 2013[48] te pessimistisch. Deze Oxford-onderzoekers keken naar de waarschijnlijkheid van het verdwijnen van beroepen in de komende twintig jaar en zagen liefst 47 procent van de Amerikaanse banen verdampen. Verschillende onderzoeken

[45] De eerste revolutie was die van de stoomenergie eind 18e eeuw; de tweede was die van de verbrandingsmotor en de elektriciteit, ongeveer een eeuw later; de derde is die van de computer en het internet van ongeveer 1960.
[46] OECD: “Policy brief on the Future of Work” (2018). Zie: http://www.oecd.org/els/emp/future-of-work/Automation-policy-brief-2018.pdf
[47] Als banen die verdwijnen noemt Richard van Hooijdonk in zijn boek onder meer: Chauffeur, boer, fabrieksarbeider, apotheker, scheidsrechter, chirurg, piloot, journalist, soldaat, bouwvakker, boekhouder en kok.
[48] Zie: https://www.oxfordmartin.ox.ac.uk/publications/view/1314

weerleggen dit maar tegelijk wijzen velen (waaronder de OESO zelf) erop dat het aantal taken dat KI niet kan, snel slinkt. De snelheid en reikwijdte hiervan zijn onbekend en dus moeten we rekening houden met verschillende scenario's.

Kader 10: Een goede aanzet voor verschillende scenario's levert het WRR-rapport "De robot de baas" uit 2015. Daarin schetsen Linda Kool en Rinie van Est negen perspectieven op werken in de robotsamenleving[49]. Ze beschrijven niet alleen dat bestaande banen verdwijnen en er nieuwe banen bijkomen (denk bijvoorbeeld aan programmeurs, designers, security-experts, virtual worlddesigners en misschien zelfs robotpsychologen en planeetbeschermers!) maar gaan tevens in op de mogelijke manieren waarop dit gebeurt.

Betekent een baanloze toekomst betaalde vrije tijd voor iedereen of juist groeiende ongelijkheid en "technologisch feodalisme"? Is de machine een complementaire collega of leidt het juist tot systeemdwang op de werkvloer? Zorgen internetplatforms voor meer ondernemerschap of juist voor digitale uitbuiting en onderbetaling? En zorgt digitalisering voor positieve specialisatie of juist voor vervreemding omdat het onderdeel van het grotere geheel steeds marginaler wordt?

De voor politici relevante vraag is dus niet of werk door KI verandert maar hoe dit gebeurt en wat dit kan betekenen voor mens en samenleving. Dit gaat over werkplezier en inkomenszekerheid maar ook over menselijke waardigheid en maatschappelijke samenhang. In dit opzicht is de ontkoppeling van productiviteit en inkomen van belang, zoals beschreven door Erik Brynjolfsson en Andrew McAfee[50], oftewel het einde van de vanzelfsprekende samenloop van industriële verdiensten en het inkomen van werknemers. De auteurs spreken van een *winner-take-all-economy* waarin een kleine groep de welvaart en de macht verzamelt om dat de winst naar de eigenaren van de technologie gaat en niet naar het collectief. Onder andere de schrijver Robert Bernard Reich wijst op technologische verdringing waarbij mensen steeds slechtere banen hebben.[51]

Niemand weet hoe de toekomst eruit zal zien en de WRR wijst er terecht op dat de impact van technologische innovaties doorgaans trager verloopt dan voorspeld en de mens zelf niet onderschat moet worden. Bovendien is technologie geen natuurkracht die ons overvalt maar iets wat we zelf kunnen vormgeven. Maar feit is dat zonder politieke bijsturing de kans groter is dat KI leidt tot een gepolariseerde arbeidsmarkt en digitale tweedeling. Wat we hoe dan ook moeten voorkomen is een toekomst waarin een algoritme-elite alles in handen heeft en zichzelf steeds verder kan ontwikkelen, verrijken en lichamelijk kan verbeteren, terwijl een grote groep mensen zonder toegang

[49] Kool en Van Est: "Kansen en bedreigingen: Negen perspectieven op werken in de robotsamenleving" (WRR, 2015)
[50] Erik Brynjolfsson en Andrew McAfee: The Second Machine Age (2014)
[51] Philipp Blom: Wat op het spel staat (2017), p. 53

achterblijft en niet meeprofiteert van de welvaartsgroei[52].

Hoe snel technologie zich ook ontwikkelt, de gevolgen voor de arbeidsmarkt verlopen meer geleidelijk. Om te voorkomen dat deze veranderingen zich buiten het politieke blikveld voltrekken is het nodig dit doorlopend te onderzoeken. Tevens is het verstandig vooruit te denken over het bijsturen en opvangen van mogelijke gevolgen op de middellange termijn. Dit vraagt onder meer om co-creatie (tussen ontwerpers en gebruikers) en complementariteit (tussen mens en machine) waarbij de mens de regie houdt[53]. Naast bescherming van werknemers op de werkvloer (veiligheid, controle, autonomie) en onderwijs (een leven lang leren, omscholing, bijscholing) moet serieus nagedacht worden over welvaartsverdeling.

D66 stelt voor:

- Doe doorlopend onderzoek naar de impact van KI op de werkgelegenheid en de inkomensverdeling.
- Geef onderwijs dat meer gericht is op toekomstige vaardigheden dan op een diploma. Zolang er nog veel terreinen zijn waarop de mens een voorsprong heeft op KI moeten we werknemers daarop laten anticiperen. Naast digitale vaardigheden zijn dit juist ook creatieve en sociale vaardigheden zoals empathie en interactie[54].
- Verdeel de welvaart. Dit kan door loonstijging of herverdeling van inkomen. Het zwaarder belasten van kapitaal, een basiscontract voor iedere werknemer of een algemeen basisinkomen bijvoorbeeld, maar denk ook aan de werknemer als mede-eigenaar van machines[55].

[52] Harari spreekt in zijn boek zelfs over een “biologische kloof” en een “upgrade van ongelijkheid” maar voor de politieke discussie heeft de tweedeling tussen een werkeloze (“nutteloze”) klasse en een technologische elite meer waarde.
[53] Went en Kremer: “Hoe we robotisering de baas kunnen blijven. Inzetten op complementariteit” (WRR, 2015)
[54] Thomas: “Anders dan zij. Onderwijs voor een robotsamenleving” (WRR, 2015)
[55] Freeman: “Wie de robots bezit, bezit de macht” (WRR, 2015)

Hoofdstuk 3. Datamacht: concurrentie en controle

Het vorige hoofdstuk heeft laten zien dat de combinatie van steeds meer beschikbare data, het internet der dingen, dataopslag in *the cloud*, supercomputers met meer rekenkracht en steeds slimmere algoritmes een revolutionaire veranderkracht betekent. Deze wordt getypeerd als de vierde industriële revolutie. Economen spreken ook wel van Industrie 4.0 of *smart industry*[56]. Net als de drie voorgaande revoluties heeft de vierde revolutie niet alleen maatschappelijke gevolgen, ook heeft de vierde revolutie zijn eigen machthebbers en monopolisten[57] gecreëerd.

Digitale markten hebben een tendens tot hoge concentratie[58]. De grote spelers bieden veel diensten aan, overstijgen daarmee bestaande marktgrenzen en worden geen marktspelers maar poortwachters. Anders gezegd: "ze concurreren niet op markten maar om markten"[59]. Daarbij zorgt de combinatie van data en algoritmes voor een zogenaamd *first-mover-advantage* en een *winner-takes-all-economy*. In de digitale economie is namelijk sprake van een sterk netwerk-effect, dat ervoor zorgt dat een product of dienst die veel gebruikt wordt in waarde stijgt. Dit effect wordt nog eens versterkt doordat de grote bedrijven hoge overstrapdrempels inbouwen en hun dienstverlening steeds verder uitbreiden (conglomeratiestrategie).

Zo zijn de techreuzen Google, Amazon, Facebook en Apple de grote industrialisten van onze tijd geworden, terwijl ook specifiekere platforms als Netflix, Spotify, Uber en Airbnb zeer machtig zijn. Al deze bedrijven maken gebruik van grote hoeveelheden data[60] en complexe algoritmes. En allemaal overstijgen ze markten en hanteren ze assertieve strategieën om dominant te blijven op hun hoofdactiviteit. Als er al een serieuze uitdager komt, dan wordt die vaak overgenomen zoals gebeurde bij YouTube en WhatsApp. Want de hoofdregel luidt: eten of gegeten worden en uiteindelijk overleeft de monopolist. Dit is niet in het belang van de concurrentieverhoudingen en dus slecht voor de consument.

---

[56] Internetdeskundigen spreken liever van Web3.0, het internet waarbij allerlei snelle internettoepassingen (media, video, audio) op elkaar worden afgestemd. Web 1.0 was overigens het web van documenten (downloaden van informatie) en Web 2.0 dat van interactie en inspraak (inclusief blogosphere)

[57] Economen en juristen zijn vaak voorzichtig met de term monopolie (1 aanbieder met verkoopmacht) en spreken liever van een oligopolie (een beperkt aantal aanbieders) of monopsonie (1 afnemer met inkoopmacht). Hoewel techreuzen als platform-poortwachters aan beide zijden van hun markten dominantie hebben en ze dus ook monopsonisten zijn, gebruiken wij steeds de term monopolisten.

[58] Er is veel aandacht voor digitale markten en hun bedrijven. The Economist wijdde er in november 2018 een special aan met de titel: "The Next Capitalist Revolution". Economisch Statistische Berichten (ESB) bracht in december 2018 een dossier "Digitale Platformen" uit.

[59] Canoy, Bruggert, Noé, Polman: "Online Platformen stellen mededingingsautoriteiten voor uitdagingen". (ESB, december 2018)

[60] Het toenemende belang van data komt ook terug in onze taal. Zie bijvoorbeeld: dataïsme, dataficatie, digitalisme

Eén van de beloftes van het internet was ooit dat producten en gebruikers vrij bij elkaar konden komen door informatie slimmer te ordenen en machtige tussenpersonen (uitgevers, platenlabels, filmindustrie) te passeren. Dat is gebeurd. 'Big Tech' heeft voor geweldige diensten gezorgd waar we dagelijks gemak van hebben, plezier van hebben en succes mee hebben. Daar hoeft de politiek weinig aan te doen. Heel anders is dat voor de nadelige consequenties van een wereld die gedomineerd wordt door digitale poortwachters die op basis van hun economische macht onze informatiestromen sturen en zo ons gedrag bepalen.

Kader 11: Machtige bedrijven die 'hun industriële revolutie' domineren zijn van alle tijden. Rond 1900 had Rockefeller's oliemaatschappij Standard Oil negentig procent van de Amerikaanse oliehandel in handen, waarbij het de hele productieketen (raffinaderijen, transport, pompstations) domineerde. Wie in die tijd olie uit de grond kon halen om zelf aan de man te brengen was machtig. Standard Oil gebruikte die macht om concurrenten uit te schakelen en prijzen op te voeren. Totdat de overheid ingreep. Gebaseerd op de Sherman Antitrust Act uit 1890 (een wet tegen concurrentieverstoring) sprak het Amerikaanse Hooggerechtshof in 1911 uit dat Standard Oil zich moest opsplitsen in 33 kleinere bedrijven.

Hoewel de Sugar Trust Case in 1895 de greep van de federale overheid op monopolievorming eerst inperkte, hebben de Verenigde Staten een rijke historie van wetgeving in het aanpakken van valse concurrentie-praktijken zoals monopolievorming, kartelvorming, handelsbeperking, prijsafspraken, boycots, fusies en verticale integratie. Zo werd bijvoorbeeld American Tobacco een kopje kleiner gemaakt en moest televisiezender NBC zich splitsen in NBC en ABC.

In zijn boek The Master Switch (2010) beschrijft de Amerikaanse professor Tim Wu hoe dit gaat in de communicatietechnologie. Dit doet hij aan de van de term Cyclus: steeds begint het met amateurs in garages of op zolderkamers die een systeem uitvinden en aanbieden, steeds eindigt het met geleidelijke concentratie en consolidatie in een monopolie, dat innovatie tegenhoudt. Op die manier kwam het telegrafie-monopolie van Western Union tot stand, gevolgd door het telefonie-monopolie van uitvinder Alexander Graham Bell (die een patentoorlog met Elisha Gray won) dat leidde tot AT&T, dat uiteindelijk ook weer gedwongen werd tot opsplitsing[61].

[61] Voor dit kader is gebruik gemaakt van het eerder genoemde boek ON/OFF van Sidney Vollmer, het discussiepaper "Tegenmacht. Liberalisme techgiganten en mededinging in de 21e eeuw" van de Mr. Hans van Mierlo Stichting, een fraai artikel van mr. M.M. Van der Wees-Hemmers van Stibbe advocaten http://www.openaccessadvocate.nl/tijdschrift/vennootschapenonderneming/2004/9/VenO_2004_015_009_007.pdf en Wikipedia-pagina's over de Amerikaanse antitrust historie: https://en.wikipedia.org/wiki/United_States_antitrust_law

De gevolgen van Big Tech

Omdat de techreuzen en internetplatforms een zodanig breed en diep bereik hebben, spelen de onwenselijke gevolgen van hun machtspositie op uiteenlopende terreinen. Alles bij elkaar zijn er vijf politiek relevante hoofdcategorieën: economische gevolgen (keuzevrijheid, concurrentie, tegenmacht), persoonlijke gevolgen (privacy en autonomie), creatieve gevolgen (afleiding en uitholling), sociale gevolgen (werkomstandigheden, verslaving en belastingmoraal) en democratische gevolgen (betwistbaarheid en beïnvloeding).

Allereerst de economische gevolgen zelf. De monopolies van het verleden beperkten de concurrentie met als gevolg hogere prijzen, minder productie, lagere kwaliteit of een combinatie van deze drie. Nu ligt dit anders want digitale consumenten betalen met data en door het netwerk-effect gaat de kwaliteit juist omhoog (daarom is de zoekmachine van Google onverslaanbaar). Toch ondervindt de consument wel degelijk economische schade.

Zo wordt de keuzevrijheid van gebruikers ingeperkt door hoge overstapdrempels. Zo zijn er geen open standaarden, zo is data moeilijk mee te nemen, zo is er geen interoperabiliteit en zo is er de steeds sturende hand van onzichtbare algoritmes. Ook dwingt de toegangspoort-werking om transacties via het grote platform te laten lopen. Verder gaat het commerciële belang van de adverteerder (die wel betaalt) uiteindelijk boven het inhoudelijke belang van de gebruiker (die gratis content benut). Daarbij misbruiken de techreuzen hun marktoverstijgende megaschaal voor praktijken als koppelverkoop of dumpprijzen om een bepaalde markt in handen te krijgen. En ze verkopen losse producten als een verplicht pakket of beperken verkoopprijzen van aanbieders, zoals Booking.com bijvoorbeeld doet richting hotels.[62]

Zo groeit hun marktmacht en zo worden ze steeds minder vatbaar voor concurrentie en innovatie[63]. Uitdagers worden weggedrukt, klein gehouden en anders opgekocht. Het consumentennadeel zit hem dus ook in de producten en diensten die de gebruiker nooit krijgt.[64]. Maar het belangrijkste is dat de economische macht van de techreuzen om meer gaat dan om economische principes. Want gezonde marktcompetitie is ook een democratisch principe. Concentraties van data, macht en geld moeten betwistbaar zijn, want macht op deze gebieden betekent ook politieke macht. Macht moet hoe dan worden ingeperkt en worden verdeeld. Macht vereist daarom tegenmacht[65].

---

[62] Haan & Overvest: "Dominatie platformen vraagt om alerte toezichthouders". (ESB, december 2018)
[63] Er wordt vaak gewezen op het feit dat Hyves verdrongen werd door Facebook en Yahoo door Google. Of dat de slachtoffers van disruptieve platforms (taxibedrijven en hotelketens) zelf hun zaakjes niet op orde hadden. Allemaal waar maar dit neemt niet weg dat de macht van de techreuzen momenteel niet wordt uitgedaagd.
[64] The Wall Street Journal schreef er vorig jaar een stevig stuk over: https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561
[65] Een belangrijke grondlegger van het idee van compenserende machten is Louis Brandeis, die van 1916 tot 1941 rechter in het Amerikaanse Hooggerechtshof was. Hij vreesde dat een kleine groep grote bedrijven buitensporig veel politieke en economische macht zou krijgen.

Dit raakt direct aan het tweede punt, onze persoonlijke privacy en autonomie. De privacy-discussie wordt al decennia gevoerd en de Europese Privacywet geeft gehoor aan de klacht dat het verzamelen en verwerken van persoonsgegevens onze persoonlijke bewegingsruimte inperkt. Maar naast privacy leveren we ook autonomie in: deels omdat we steeds afhankelijker worden van digitale diensten en producten van Facebook en Apple. En deels omdat onze toegang tot en selectie van informatie, zoals artikelen, muziek en advertenties ons op basis van dataprofielen en algoritmes aangeboden worden. Dit wordt bepaald door de techreuzen. Grotendeels zonder dat we dit weten en veelal zonder dat we dit vragen[66].

Dan de creatieve gevolgen, want die zijn er ook. Iedereen weet hoe het is om voortdurend afgeleid te worden door zijn smartphone vol applicaties en hun eindeloze notificaties. Ook de werk-privé-balans is tegenwoordig zodanig verstoord dat er na het recht om vergeten te worden nu nagedacht wordt over het recht om onbereikbaar te zijn. Hoewel het verslavend kan werken, is dit ook ieders eigen verantwoordelijkheid. Leg je telefoon weg, zet die meldingen uit en reageer gewoon niet altijd direct.

Dit ligt anders bij de positie van schrijvers, muzikanten en andere ambachtelijke makers die steeds minder voor hun creaties krijgen. In zijn bijtende boek "Ontzielde wereld" zet Franklin Foer[67] uiteen hoe Amazon-baas Jeff Bezos het boek uitkoos als beste product om daar zijn online winkel mee te beginnen. Inmiddels is Amazon een online winkel met een soort kennismonopolie. De bijhorende marktmacht (inkoopmacht) van dit bedrijf is de reden dat een e-boek 9,99 dollar kost. Amazon zet uitgevers onder druk en schrijvers verkopen steeds minder boeken, voor een steeds lagere prijs. In de muziekwereld hebben iTunes en Spotify voor een vergelijkbare beweging gezorgd, een vorm van broodroof waartegen steeds meer muzikanten in opstand komen. Ook hier geldt dat de grote artiesten het wel redden via bijvoorbeeld fanshops en concerten, maar de rest moet sappelen.

In het verlengde hiervan liggen de sociale gevolgen. Hoewel de sprankelende campussen en hip ingerichte gebouwen van Google de inspiratie waren voor het internetsprookje van Dave Eggers over droombedrijf The Circle[68], is de realiteit anders. De werkomstandigheden bij de grote Techreuzen zijn berucht. De contentmoderators bij Facebook, het Chinese fabriekspersoneel bij Apple, de magazijnmedewerkers bij Amazon, maar ook de onderbetaalde chauffeurs bij Uber zijn verontrustende voorbeelden. Deze voorbeelden geven de ontkoppeling tussen productiviteit en inkomen aan.

[66] Onder veel anderen wijzen schrijvers als Dimitri Tokmetzis, Andrew Keen, Bruno Latour, Evgeny Mozorov, Franklin Foer, Hans Schnitzler en Sidney Vollmer hier alle op in hun boeken.
[67] Franklin Foer: Ontzielde wereld (2017), H4.
[68] Dave Eggers, The Circle (2015)

Een ander punt dat de samenleving raakt is de beroerde belastingmoraal van de techreuzen. Onlangs werd de waarde van Apple en Amazon berekend op 1 biljoen. Deze bedrijven hebben een jaaromzet die veel Europese landen overstijgt. Op zichzelf is daar niets mis mee maar hun grote schaal en digitale vorm wordt gebruikt om belasting te ontwijken[69]. Multinationals betalen belasting over de winst in het land waar ze fysiek gevestigd zijn en de techreuzen in de EU vestigen zich daarom in fiscaal aantrekkelijke landen zoals Ierland en Luxemburg. Op die manier hoeven zij over hun omzet in Nederland bijvoorbeeld haast geen belasting betalen. Dit zorgt voor minder inkomsten voor publieke voorzieningen en voor frustratie in de samenleving. Tot slot zijn er nog lokale en sectorale nadelen zoals de ontwrichting van stedelijk woningmarkten door Airbnb en de verslaving die de game-industrie veroorzaakt.

Ten slotte de democratische gevolgen. De gebeurtenissen tijdens de laatste verkiezingen in de Verenigde Staten en de rol van Facebook daarbij hebben desinformatie en nepnieuws definitief op de agenda gezet. De verantwoordelijkheid voor het oplossen van deze vorm van buitenlandse inmenging via social media ligt voor een groot deel bij de platforms zelf. Het schrijnende is dat de traditionele journalistiek hierbij moet helpen vanwege hun ervaring met factchecking, redactiestatuten en ombudsmannen. Schrijnend, omdat de advertentiemacht van Google, Facebook en Amazon de onafhankelijke journalistiek in het digitale tijdperk juist een zware slag heeft toebedeeld. En daarmee ook hun rol als controleur van de democratie. Steeds vaker worden journalisten gedwongen te kiezen voor laagdrempelige verhalen in plaats van tijdrovende onderzoekjournalistiek. En dat terwijl niemand hier beter van wordt, want betwistbaarheid van informatie, kennis en macht is een hoeksteen van onze vrije samenleving. Dit bespreken we in hoofdstuk vier.

Kader 12: Er zijn talloze boeken en artikelen geschreven over de nadelige gevolgen van de techreuzen, zoals hierboven kort beschreven. De kritiek daarop is vaak dat het eenzijdig gericht is op de negatieve kanten, selectief onderbouwd en schromelijk overdreven. Daar zit absoluut een kern van waarheid in en sommige aspecten zijn inderdaad vergezocht of worden aangedikt. Toch is het belangrijk om kritisch te kijken naar het gedrag van de techreuzen. Het is onmiskenbaar dat ze de grootste en machtigste bedrijven zijn van onze tijd. Hun geld, producten en diensten, maar ook hun uitstraling, innovatie- en lobbykracht geeft ze veel invloed in onze samenleving hetgeen nauwelijks kan worden onderschat. Hun diensten en hun verhalen over verbinding en verbetering zijn verleidelijk, terwijl hun eigen daden, doelen en activiteiten schimmig zijn. Elke politicus heeft de morele plicht om hier met argusogen naar te kijken en mensen te beschermen tegen de onwenselijke consequenties van vandaag en morgen. Dat moet zo evenwichtig en feitelijk mogelijk, gebaseerd op concrete feiten en voorbeelden. En niet op basis van doemscenario's en angstbeelden.

[69] Jeff Bezos wilde Amazon bijvoorbeeld in een Indianenreservaat in Californië huisvesten om haast geen belasting te hoeven afdragen. Ook probeerde hij elke gebondenheid aan een staat te verhullen.

Tijd om in te grijpen

Op basis van het bovenstaande is er genoeg reden om in te grijpen bij het ongewenste gedrag van de techreuzen. Dat inzicht is allesbehalve nieuw en wordt steeds breder gedeeld. Maar waarom gebeurt er dan nog relatief weinig?

Allereerst beschouwen nationale overheden deze bedrijven niet als *Too Big To Fail* maar als *Too Big To Miss*. Bovendien zijn ze grenzeloos, niet gebonden aan plaats, grens of tijd. Dat weerhoudt politici van actie, omdat zij zich wel aan geografische grenzen moeten houden. De moeizame aanpak van Pirate Bay liet dit zien: iedereen zag dat 'illegaal downloaden' niet eerlijk was, maar daar bleef het bij omdat elke ingreep ook nadelen had. Ingrijpen in de complexe (en onzichtbare) digitale wereld van internetdiensten, big data en algoritmes is niet eenvoudig. Als het niet is vanwege een gebrek aan kennis, snelheid of prioriteit, dan is het wel door een gebrek aan goede wettelijke instrumenten.

Veel bestaande wetgeving is niet toegesneden op de nieuwe wetten van de digitale economie. De voor het mededingingsrecht relevante markten zijn bijvoorbeeld niet scherp gedefinieerd. Dat komt doordat de techreuzen zich vaak grote delen van de productieketen toe-eigenen, ook wel verticale integratie genoemd. Iets waar Google en Amazon zo bedreven in zijn dat The Economist zelfs schreef dat deze bedrijven niet opereren in een markt, maar de markt *zijn*[70]. En als politici dan toch een wet maken, dan is de intentie vaak beter dan de uitvoering. Gebruikers krijgen namelijk te maken met negatieve gevolgen, zoals cookiemeldingen, of bedrijven omzeilen de wetten eenvoudig door geen expliciete toestemming te vragen [71].

Maar hoe moeilijk ook, reguleren is wel nodig. Daarom doen we voorstellen op verschillende wetgevingsdomeinen. Waar de situatie vraagt om een specifieke of snellere aanpak, op nationaal niveau. En wanneer samenwerking geboden is, op Europees niveau.

Geen nutsbedrijf, zorgplicht of megawet

In de discussie over de techreuzen en internetplatforms vallen vaak drie termen. De eerste is "opknippen", op basis van de historische vergelijking met Standard Oil, AT&T en Microsoft. De gedachte is dat de markt faalt en dat de overheid de markt moet bijsturen. Daar gaan we straks op in.

[70] The Economist, 18 januari 2018: "Competition in the digital age. How to tame the Tech titans?"
[71] Een treffend voorbeeld hiervan is de terecht geïnitieerde maar mislukte cookiewet.

De tweede term, bijna tegenovergesteld hieraan, is “nutsbedrijf”. Deze term wordt door Mark Zuckerberg zelf gebruikt. Men maakt dan al snel de sectorale vergelijking met publieke voorzieningen zoals energie en water, die ook gedeeltelijk in handen van de staat zijn. De gedachte daarbij is dat de betreffende diensten van algemeen belang zijn, wat overheidsingrijpen rechtvaardigt. In het verlengde hiervan valt ook vaak de term “zorgplicht”, of bijsluiter. Dit op basis van de vergelijking met de bankensector die met onduidelijke financiële producten, zoals hypotheekproducten en derivaten de consument benadeelde en het dus beter moest uitleggen. Waarom zou dit niet gelden voor digitale diensten met hun onzichtbare algoritmes en ellenlange gebruiksvoorwaarden?

Het zijn aardige gedachten, maar moeilijk politiek vertaalbaar. Je kunt denken aan een veilige publieke versie als alternatief voor Facebook, dus met alle mogelijkheden maar zonder de gepersonaliseerde advertenties en eventueel tegen betaling. Of Google tot nutsdienst maken en de zoekmachine gereguleerd aanbieden. Of het online platform van Amazon onder voorwaarden beschikbaar stellen voor andere aanbieders. Ondenkbaar is het allemaal niet, maar voor we als overheid het werk van bedrijven gaan overnemen of privaat eigendom gaan doorkruisen, verdienen andere ingrepen de voorkeur.

Een derde term is die van een allesomvattende “datawet”. In de Verenigde Staten hebben de Democraten voorzichtige stappen gezet in de richting van een “*Internet Bill of Rights*” met tien principes over data[72]. In Nederland pleitte de PvdA ooit voor een datawet. Sympathieke voorstellen maar het probleem is dat een alles-in-een-aanpak ondoenlijk is omdat data (net als geld) op vele gebieden een rol speelt. Daarom kiezen we hier evenmin voor.

Competitie en concurrentie

D66 beschouwt het mededingingsrecht als meest directe en dus meest aangewezen route om de dominantie van de techreuzen te begrenzen. Het idee is om meer concurrentie af te dwingen door het mededingingsrecht aan te passen aan het digitale tijdperk. Dit is nodig “omdat het in zijn huidige vorm niet is bedoeld als instrument om succesvolle ondernemingsdrift te straffen door afstoting of opsplitsing af te dwingen”, aldus hoogleraar Mededingingsrecht Anna Gerbrandy[73] in NRC. De juridische grondslag bestaat wel maar de Europese Commissie zal dit alleen inzetten als het niet anders kan. Een andere beperking is dat data –“het nieuwe goud, de nieuwe olie, de grondstof van de digitale economie”- geen plek heeft in het mededingingsrecht.

[72] Een aantal van deze principes is in Europa al geregeld via de AVG en andere wetgeving.
[73] https://www.nrc.nl/nieuws/2017/05/05/macht-van-google-is-groot-maar-wettelijk-niet-verboden-a1557357

Dit is de reden dat veel economen het mededingingsrecht niet zien als het instrument voor het aanpakken van de techreuzen[74]. In navolging hiervan bewandelen ook politici vooral niet-economische wegen om de *gevolgen* van marktmacht te beteugelen. De marktmacht *zelf* blijft zo in tact. Denk hierbij aan de Europese inzet op privacywetgeving (de AVG en de ePrivacy verordening), auteursrecht (een uploadfilter en een linktaks), beteugeling van nepnieuws (platformverantwoordelijkheid en advertentieregels) of belasting (digitaks). Op zich prima om te bekijken maar allemaal meer symptoombestrijding dan marktgenezing.

De tijd is rijp om ook mededinging zelf in te zetten tegen digitale marktmacht. Gelukkig kijkt de Europese Commissie onder leiding van Eurocommissaris Vestager naar competitie in de digitale economie. Maar in Europa is mededinging een gecombineerde taak van de Unie en de lidstaten met hun nationale wetgeving en toezichthouders. Daarom komt D66 met de initiatiefnota "Mededinging in de Digitale Economie".

D66 stelt voor:

- Pas de relevante artikelen uit het Europees Verdrag en daaraan gekoppelde verordeningen aan. Dit biedt openingen voor de Europese mededingingswetgeving en de Nederlandse Mededingingswet. Geef data een plek in mededinging en maak markten daardoor beter te beoordelen op machtsmisbruik.
- Erken data als essentiële faciliteit (onmisbare productie-input) waarbij externe toegang en data-delen kan worden afgedwongen om concurrentie te bevorderen.
- Stel een Europese, niet politiek-gestuurde, toezichthouder in die toegang krijgt onder de motorkap van digitale bedrijven en die sancties kan opleggen
- Breid het concentratietoezicht uit met een beoordelingscriterium 'data'. Beschouw data als vermogensbestanddeel waardoor bij horizontale en verticale fusies beter kan worden beoordeeld wat de effecten zijn voor de markt.
- Geef hogere boetes bij machtsmisbruik. De recente EU-boete van 4,34 miljard euro[75] lijkt veel maar op een jaaromzet van ruim 100 miljard schrikt het onvoldoende af.
- Verduidelijk bestaande en bruikbare marktordeningsregels (bijvoorbeeld om de positie van platforms beter te kunnen beoordelen) zodat ze beter kunnen worden toegepast in digitale markten.

[74] Wiedijk en van Dongen wijzen in hun ESB-artikel "Opties om een competitieve digitale economie te behouden" (2018) bijvoorbeeld op regulering in de vorm van verplichte neutraliteit in rangordes, het reguleren van tarieven of het dwingen tot datadelen.

[75] https://tweakers.net/nieuws/141097/eu-legt-google-recordboete-van-4-komma-34-miljard-euro-op-om-android-machtsmisbruik.html

Privacy en persoonsgegevens

Op basis van een sociale en ethische invalshoek heeft Europa als economische wereldmacht de kans om zich te onderscheiden van enerzijds het relatief regelloze marktkapitalisme van de Verenigde Staten en anderzijds de centraal geleide staatseconomie van China. Dit door data als kritische massa van de interneconomie beter te reguleren.

Omdat de techreuzen steeds meer data over jou en je omgeving verzamelen en verwerken tot profielen[76], krijgen zij steeds meer kennis en controle over je leven. Nu gebeurt dit nog via '*trackers*', maar in de toekomst wordt koopgedrag grotendeels geautomatiseerd. De waarde van onze data neemt daardoor toe en de vraag van wie die data nu eigenlijk zijn, wordt steeds belangrijker. Over die vraag (de definitie van data, persoonsgegevens, eigendom van deelbare informatie, enzovoorts) breken vele deskundigen al lang het hoofd. De wetenschap is hier niet uit en tot die tijd is het aan politici. Op het gebied van privacy en persoonsgegevens hebben ze die verantwoordelijkheid nu genomen in de vorm van de Privacywet AVG. Deze moet nu zijn waarde gaan bewijzen, samen met de aanstaande ePrivacy-verordening[77]. Deze gaat het bijvoorbeeld mogelijk maken om van het internet gebruik te maken zonder data te hoeven delen, wat een grote stap voorwaarts is. Algoritmes worden hiermee echter niet voldoende gevangen. Daarom is er meer nodig.

D66 stelt voor:

- **Informeer burgers actief over hun toegenomen mogelijkheden tot regie over hun eigen persoonsgegevens. De AVG vergroot de privacy en breidt de rechten van burgers uit. Zowel achteraf (de reeds verzamelde data), als vooraf: zonder toestemming mogen bedrijven geen nieuwe data verzamelen.**
- **Geef burgers via de e-Privacy verordening het recht om beperkt data te delen en verplicht bedrijven om gegevens apart te behandelen, zodat deze niet aan elkaar gekoppeld worden. Dit gebeurt nu bij Facebook, WhatsApp en Instagram of bij Google, YouTube en Gmail maar ook bij de Nederlandse Persgroep en bij Talpa-SBS.**

[76] Dat dit flinke vormen aanneemt bleek uit onderzoek in 2015: https://www.volkskrant.nl/wetenschap/na-150-likes-kent-facebook-je-beter-dan-je-beste-vriend~bff6823f/

[77] De Europese Unie onderhandelt momenteel over de e-Privacy verordening. D66 heeft het kabinet via de motie Verhoeven opgeroepen om dit punt te bepleiten namens Nederland.

- Laat de algoritme-waakhond algoritmes en onderliggende data controleren. Maak tempo met het digitale team van de Autoriteit Consument en Markt en met de extra middelen die de Autoriteit Persoonsgegevens meer digitale slagkracht geven[78].
- Beoordeel nieuwe technologieën zoals Virtual Reality/Augmented Reality direct op hun privacy-consequenties. De vraag hierbij is of en hoe bestaande wetgeving dit goed afdekt. Deze technologieën moeten zich strikt beperken tot de doelen waarvoor ze ingezet worden.
- Laat alle proeven met gezichtsherkenning, herkenning in de openbare ruimte door overheden, opsporingsorganisaties of andere semioverheidsinstellingen vooraf goedkeuren door de minister van Justitie en Veiligheid.
- Maak budget beschikbaar voor alternatieven die burgers op het internet beschermen. Zoals de QIY foundation, een organisatie die consumenten meer controle geeft over hun digitale gegevens, ofwel hun online identiteit.

Belasting betalen en opbrengst delen

Dat de techreuzen hun belastingplicht via allerlei constructies grotendeels ontlopen is steeds meer politici een doorn in het oog. De Europese Unie werkt daarom aan een voorstel voor een zogenaamde digitaks, waardoor ze belasting moeten gaan betalen over de omzet die ze in een lidstaat generen. Dit voorstel beperkt zich tot verdiensten uit advertenties en laat dataverkoop en intermediaire diensten (platforms) vooralsnog buiten beschouwing. Frankrijk wil dit al sinds 2012 en de Franse minister Le Maire van Economische Zaken heeft recent gezegd het zelf in te voeren als de EU er voor 1 maart 2019 niet uit is. Het Verenigd Koninkrijk gaat hetzelfde doen in april 2020. Hoewel het Europees Parlement het voorstel van de Commissie met grote meerderheid steunde, ligt het gevoelig in de Europese Raad waar verschillende lidstaten, met elk een (belasting)veto, dwarsliggen.

Deels is het de eigen verantwoordelijkheid van mediabedrijven en auteurs om een eerlijke prijs voor hun product te krijgen. Vraag geld voor je content zoals steeds meer mediabedrijven doen. Een andere manier is aanpassing van het auteursrecht. Net zoals de antitrust-wetgeving kent dit recht een roemruchte geschiedenis daterend uit de tijd van de boekdrukpers. In het boek de Ontzielde Wereld introduceert Franklin Foer[79] de heer William Wordsworth. Een man die zijn leven lang streed voor auteursrecht in de VS. Toen het er eindelijk kwam, vergaten de wetgevers echter om buitenlandse boeken eronder te laten vallen, zodat vele illegale kopieën van Britse

[78] Afgelopen jaren heb ik allerlei creatieve suggesties gehoord en gelezen voor een toezichtsorgaan op het gebied van data. Zoals de Nationale Digitale Autoriteit (Sidney Vollmer), Het Centraal Bureau voor de Internetstatistiek of de Algemene Datakamer.
[79] Franklin Foer: Ontzielde Wereld (2017), p. 193

schrijvers in de VS verschenen. Pas toen dit gat gedicht werd, ontstond er Amerikaanse literatuur. Zo belangrijk is bescherming van intellectueel eigendom dus. Een aardige suggestie die hieraan raakt, komt van Sidney Vollmer, die pleit voor aanpassing van het auteursrecht richting de octrooiwetgeving in de farmaceutische industrie[80]. Dat duurt geen 70 jaar door na de dood van de bedenker, maar slechts twintig jaar.

D66 stelt voor:

- **Voer als Nederland de druk in de Europese Raad op zodat de digitaks er zo snel mogelijk komt. Zo niet, volg dan het voorbeeld van Frankrijk en Oostenrijk en voer het zelf in.**
- **Ga selectief gedrag van bedrijven tegen. Door harmonisatie, of op zijn minst een minimale EU-standaard voor een aantal Europese belastingen. Het bestrijden van de fiscale race naar de bodem kan enkel en alleen in Europees verband.**
- **Pas het auteursrecht aan, bijvoorbeeld door computercode erin mee te nemen of door de werkingstermijn van 70 jaar te verkorten. Geen linktaks en uploadfilters.**
- **Stimuleer als overheid open source software, bijvoorbeeld door algoritmes niet onder het bedrijfsgeheim te laten vallen.**

Goed gedrag

Toen Uber in Nederland de markt opkwam, deden ze dat met een uiterst assertieve strategie. Het bedrijf was zo 'disruptief', dat ze niet aan ouderwetse (taxi)wetten konden voldoen. En dus overtraden ze de wet, "in het belang van de burger". Hoewel het spanningsveld tussen wetgeving en innovatie evident is, was dit te gortig. En dat vond de inspectie ook. UberPop werd in Nederland verboden, zoals in vele Europese steden. Het overtreden van wetten en onderbetalen van werknemers liep tegen politieke grenzen op.

Hetzelfde geldt voor Airbnb, het platform dat het mogelijk maakt je woning te verhuren als hotelkamer. In veel steden waaronder Amsterdam leidde dit verdienmodel voor huiseigenaren tot een dusdanige ontwrichting van de hotelmarkt en de woningmarkt dat het college van B&W besloot in te grijpen. De verhuurtermijn werd gemaximeerd tot 30 dagen per jaar[81]. Deze voorbeelden laten zien dat het grenzeloze en onafhankelijke karakter van internetbedrijven relatief is. Omdat de juridische aansprakelijkheid in de deeleconomie vaak onduidelijk is en bedrijven niet dwingt tot het nemen van verantwoordelijkheid, moeten politici en toezichthouders waar nodig optreden. Naast Europese en nationale ingrepen, zijn soms sectorale en lokale ingrepen nodig.

[80] Sidney Volmer: ON/OFF (2017), p. 284
[81] RTL Nieuws: https://www.rtlnieuws.nl/nederland/artikel/3801246/amsterdam-legt-airbnb-verder-aan-banden-tot-30-dagen-jaar

D66 stelt voor:

- Treed als gemeente, toezichthouder of inspectie actief op bij overtreding op je gebied of domein. Juist als de gevolgen lokaal of sectoraal zijn[82].

[82] Een mooi voorbeeld is Veilig Verkeer Nederland dat in gesprek wil met taxidienst Uber, webwinkel Coolblue en boodschappenbedrijf Picnic over het rijgedrag van hun chauffeurs. (Volkskrant, 19 januari 2019)

Hoofdstuk 4. Cyberstrijd: aanvallen afslaan

Cybersecurity wordt steeds belangrijker omdat onze samenleving steeds afhankelijker is van digitale technologie. Of het nou gaat om energienetten, sluizen en dammen, waterzuiveringsinstallaties, ziekenhuisapparatuur, auto's, thermostaten, fabrieken of financiële transacties. Elk aspect van ons leven is doordrongen van digitale technologie. Dat betekent dat de veiligheid van die technologie en de weerbaarheid tegen aanvallen ook steeds belangrijker wordt. Bovendien ziet de AIVD digitale aanvallen als een van de grootste dreigingen waar Nederland mee te maken heeft[83] en stelt de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) dat deze dreiging toeneemt[84].

Dat er afgelopen jaren meer aandacht en geld voor cybersecurity is gekomen, is waardevol. Ook is het van belang dat het Nationaal Cybersecurity Centre (NCSC) is versterkt, het Digital Trust Center (DTC) is opgezet, de mogelijkheid van een nieuw Cybersecurity-onderzoeksinstituut wordt onderzocht, onveilige IoT-apparaten[85] meer aandacht hebben gekregen en een beter digitaal bewustzijn wordt aangewakkerd.

Maar deze nationale inzet neemt niet weg dat digitalisering bij uitstek een grensoverschrijdend fenomeen is en dat de wereld steeds meer een toneel wordt van cyberstrijd in de vorm van buitenlandse beïnvloeding, desinformatie, digitale aanvallen, economische spionage, een technologische wapenwedloop en zelfs *cyberwarfare*. Dit vraagt om een alerte opstelling en een internationale strategie. Hierbij onderscheiden we vier hoofdthema's.

Desinformatie

Zorgen over misleidende media zijn van alle tijden. Bij grote veranderingen van het medialandschap was er telkens argwaan over de effecten van het toenemende bereik. Dat was zo bij de telegraaf, de drukpers, de radio, de tv en nu bij het internet. Overheden hebben altijd regulering toegepast.

Bij het internet zou ingrijpen echter lastig zijn, omdat het de beloofde vrijhaven is waarin iedereen gelijk is. Het zou "een andere wereld" zijn, waarbij regelgeving te ingewikkeld is om te ontwerpen. Terwijl traditionele media

[83] AIVD: https://www.aivd.nl/onderwerpen/cyberdreiging/digitale-beinvloeding
[84] NCTV: Cybersecuritybeeld Nederland 2018
[85] Zie voor de D66-inzet aangaande het internet der dingen onze initiatiefnota uit 2016: https://d66.nl/verkoopverbod-onveilige-internetapparaten. In haar advies ' Naar een veilig verbonden digitale samenleving' bevestigde de Cyber Security Raad (CSR) het belang van deze maatregelen in 2017.

gesloten kanalen zijn met een eindredactie, biedt het internet de mogelijkheid van open kanalen waar iedereen zijn eigen nieuwskanaal kan starten. Alle berichten gaan ongecontroleerd de wereld in. Ook zijn de omgangsvormen op sommige social media platforms verre van vrolijk makend en plaatsen (anonieme) trollen en bots agressieve, beledigende en bedreigende reacties[86].

De (pogingen tot) beïnvloeding van presidentsverkiezingen in de VS en Frankrijk, maar ook de referenda over Brexit en het Oekraïne-verdrag hebben aangetoond dat het internet geen afgescheiden ruimte van de realiteit is. Er is geen dualisme zoals sommigen pretenderen, er is geen digitale wereld én een wereld daarbuiten. Het internet maakt onderdeel uit van de publieke ruimte. Dat legitimeert regulering indien de situatie daarom vraagt. Wetgeving gaat te ver omdat dit leidt tot een overheid die bepaalt wat waar is en zelfs censuur. De mislukte werkwijze van de Europese instantie EU vs Disinfo onderstreepte dit. Maar andere maatregelen zijn heel goed mogelijk.

D66 stelt voor:

- Organiseer een bewustwordingscampagne voor de twee verkiezingen in 2019 en doe onderzoek naar de impact van desinformatie tijdens deze verkiezingen.
- Stimuleer samenwerking tussen traditionele media en social media platforms waarbij het checken van feiten en onderzoeksjournalistiek centraal staan.
- Laat Google, Facebook en Twitter hun verantwoordelijkheid nemen door transparanter te zijn over hun advertentie- en contentbeleid en de werking van hun algoritmes.
- Laat diensten en advertenties herleidbaar zijn naar een rechtspersoon die aanspreekbaar en aansprakelijk is. Misleiding is strafbaar dus handhaaf dit beter. Zet ook in op actievere detectie van trollen en bots.
- Anoniem deelnemen aan discussies op open platforms en publieke fora moet kunnen[87]. Maar verwijder accounts die misbruik maken. Privacy is een groot goed maar mag nooit misbruikt worden om online mensen aan te vallen.

[86] Toen de Leidse politicoloog Rebekah Tromble onderzoek deed naar de omgangvormen op Twitter, werd zij bedolven onder tienduizenden hatelijke commentaren en doodsbedreigingen. (Volkskrant, 12 januari 2019)
[87] Technisch moet je sowieso geen beperkingen aanbrengen die anonimiteit aantasten (zoals backdoors). Maar dit neemt niet weg dat mensen zelf fouten maken en daardoor toch herleidbaar zijn. Een andere vraag is: anoniem voor wie en in welke mate? Hier gelden uiteindelijk wel bepaalde grenzen, die er ook in de fysieke wereld zijn.

Digitale aanvallen

De recente aanval van Russische staatshackers op de Organisatie voor het Verbod op Chemische Wapens (OPCW), de poging om de Onderzoeksraad voor Veiligheid te hacken, de ransomware aanvallen Wannacry en NotPetya, de hack op de Franse zender TV5Monde, de cyberaanval op de Duitse Bundestag, de Russische aanval op de Democratische partij (DNC): hoe verschillend van aard en oorzaak ook, alle gevallen laten zien hoe belangrijk goede cybersecurity en veilige software is[88].

Dit begint bij beter bewustzijn, en de basis op orde brengen: goede wachtwoorden gebruiken, 2-factor-authenticatie, niet op verdachte links klikken, tijdig beveiligingsupdates installeren en verbindingen versleutelen. Vaak zijn de grootste cyberaanvallen geen kwestie van *high tech* maar van *low-tech*: mensen die op een link klikken of in een (spear)phishing aanval trappen. Overigens kunnen ook falende mailservers of spamfilters een reden zijn van een succesvolle cyberaanval.

Een tweede aandachtspunt is het snel groeiende Internet of Things (IoT). Dit creëert nieuwe verantwoordelijkheden voor producenten. Gehackte apparaten in bijvoorbeeld woningen of logistieke systemen vormen een steeds groter veiligheidsrisico. Voor individuele gebruikers, maar ook voor de maatschappij als geheel, bijvoorbeeld als grote hoeveelheden gehackte apparaten ingezet worden voor DDoS-aanvallen op banken of overheidswebsites. In het regeerakkoord is hier aandacht voor. Het kabinet zet in op verplichte minimumeisen en certificering voor op internet aangesloten apparaten, en het aansprakelijk stellen van producenten die nalatig zijn.

Het organiseren van samenwerking en het delen van kennis over aanvallen is een derde onderdeel van een complete cybersecurity-aanpak. Binnen het Nationaal Cyber Security Centrum (NCSC) komen organisaties en bedrijven uit vitale sectoren samen om informatie uit te wisselen[89]. Daarbij is de cybersecurity-wet aangenomen die aanbieders van essentiële diensten, zoals drinkwaterbedrijven of banken verplicht te voldoen aan bepaalde veiligheidseisen. Bovendien heeft Nederland als een van de eerste landen ter wereld een zogeheten *Responsible Disclosure* richtlijn die ethisch hackers in staat stelt om veilig kwetsbaarheden te melden. Nederland loopt voorop en het is zaak die voorsprong te behouden.

Ten vierde een paradoxaal punt, te weten defensie en de inlichtingen- en opsporingsdiensten die bij hun werk

[88] Ook recent waren Duitse politici doelwit van een hackaanval. Hackers verspreidden gegevens van honderden politici online, vanuit het twitteraccount 'G0d' (19 duizend volgers)
[89] Nederlandse bedrijven werken ook samen om digitale aanvallen zo goed mogelijk op te vangen. Een voorbeeld is de Dutch Continuity Board dat diensten bereikbaar houdt tijdens DDoS-aanvallen: https://www.dcboard.nl/about-us

voor de nationale veiligheid gebruik (mogen) maken van zogenaamde *zero-day exploits*: softwarefouten waar cyberwapens van gemaakt kunnen worden. Het voordeel hiervan is dat ze verdachten of targets kunnen volgen, het nadeel is dat deze softwarefouten dus niet gemeld en gedicht worden, zodat ze ook door kwaadwillenden (hackers, statelijke actoren) gebruikt kunnen worden[90] en dus vitale infrastructuur of andere apparaten onveilig houden.

De paradoxaliteit is dus dat veiligheidsorganisaties het internet onveilig kunnen maken bij onverantwoordelijk gebruik van zero-days. In de Verenigde Staten is daarom het zogeheten *Vulnerabilities Equities Process* opgezet dat verschillende diensten en ministeries bij elkaar brengt om te beslissen of een bepaalde zero-days gebruikt of gedicht moeten worden. In Nederland is een dergelijk afwegingskader via een beleidsregel van toepassing op de AIVD en MIVD, maar de politie en defensie onttrekken zich hieraan. D66 wil het afwegingskader voor het gebruik van zero-days door overheden wettelijk regelen via een initiatiefwet[91].

D66 stelt voor:

- Maak een wettelijk afwegingskader voor cyberwapens op basis van zero-days. Stop met de inkoop van hacksoftware of zero-days die niet openbaar gemaakt worden vanwege bedrijfsgeheim of intellectueel eigendom.
- Houd vast aan het standpunt dat encryptie niet verzwakt mag worden voor opsporingsdoeleinden. Breng de gevolgen van quantumcomputing voor encryptie (op staatsgeheimen en intellectueel eigendom) in kaart. Start een 'Quantum-safe' agenda om overheden en bedrijven voor te bereiden op quantum supremacy.
- Leg meer nadruk op preventie. Geef ambtenaren en medewerkers in gevoelige sectoren zoals transport, energie en het bankwezen training in digitale veiligheid.
- Stimuleer 2-factor-authenticatiesystemen (in plaats van gebruikersnaam en wachtwoord), wachtwoordmanagers, het herkennen van verdachte links, goede versleuteling en tijdige software-updates[92].
- Lanceer een deltaplan voor cyberveiligheid in de vitale infrastructuur om kwetsbaarheden in kaart te brengen en aan te pakken.

[90] Dit gebeurde bij de Wannacry-aanval die gebruik maakte van een kwetsbaarheid die de NSA had ontdekt en die werd gekaapt door de hackersgroep Shadow Brokers)
[91] Deze initiatiefwet is eind 2018 aangekondigd: https://nos.nl/artikel/2264338-strengere-regels-nodig-voor-hacks-door-overheid-via-zero-day-bugs.html
[92] Onderzoeker Brenno de Winter wijst erop dat slechte digitale hygiëne en herhaalfouten de grote gemene deler zijn bij de ruim 2.000 datalekken die hij onderzocht. Hij pleit voor een beveiligingskadervergelijkbaar met het Safety of Life at Sea verdrag (SOLAS)

- Introduceer een omgekeerde bewijslast (*due dilligence*) voor digitale veiligheid. In het geval van incidenten moet een organisatie aantonen dat haar veiligheid op orde was, in plaats van dat aangetoond moet worden dat het tekort schoot. Laat incidenten onderzoeken, bijvoorbeeld door de Onderzoeksraad voor Veiligheid (OVV).
- Verplicht grote bedrijven een hoofdstuk in hun jaarverslag te wijden aan cybersecurity. Geef cyberveiligheid een grotere rol in aanbestedingen.
- Laat ministeries rapporteren over systemen die draaien op verouderde software (*legacy*). Creëer een beloningsstructuur voor ethisch hackers en onderzoekers die zwakke plekken ontdekken. Leg het *responsible disclosure* principe wettelijk vast zodat ethische hackers niet strafrechtelijk vervolgd worden.
- Kom vooruitlopend op Europese minimumeisen en een marktverbod voor slecht beveiligde IoT-apparaten met een nationale aanpak via een keurmerk of certificering en een verstevigd aansprakelijkheidsrecht.

Technologische wapenwedloop

Een paar maanden geleden besloot de minister van Justitie en Veiligheid dat de Nederlandse overheid stopt met het gebruik van Kaspersky Antivirussoftware[93]. Het risico op spionage was te groot. Deze voorzorgsmaatregel werd onderbouwd op basis van drie argumenten. Namelijk dat bedrijven als Kaspersky de Russische inlichtingendiensten zouden ondersteunen in hun taken, dat de Russische federatie een offensief cyberprogramma heeft dat ook gericht is op Nederland en dat de software van Kaspersky diep in onze systemen zit.

Dit voorbeeld staat niet op zichzelf. Steeds vaker vraagt de modernisering van systemen om cruciale specifieke technologieën die Nederland (of Europa) niet zelf maakt. Deze technologie moet dan worden ingekocht maar het probleem is dat in de buitenlandse hard- en software achterdeurtjes (*backdoors*) kunnen zijn ingebouwd, waardoor kan worden meegekeken of waarmee informatie kan worden weggesluisd[94]. Andere recente gevallen zijn de 5G[95]-technologie van het Chinese bedrijf Huawei en het C2000-communicatiesysteem van Hytera Mobilfunk, een Duitse dochteronderneming van het Chinese Hytera. In beide gevallen vroeg de Tweede Kamer om uitleg vanwege de risico's van de productafhankelijkheid voor onze vitale infrastructuur en cruciale overheidsprocessen. In reactie hierop werkt het kabinet aan zowel een China-strategie als een Rusland-strategie.

[93] Zie: https://www.nrc.nl/nieuws/2018/05/14/kabinet-stopt-met-russische-antivirussoftware-van-kaspersky-a1602901
[94] Als dit al nodig is. Toegang tot systemen lukt vaak ook via bestaande technologie of via onderhoudscontracten
[95] 5G staat voor vijfde generatie mobiel internet dat de huidige generatie (4G) vanaf 2020 moet vervangen en dat veel sneller is en bijvoorbeeld de groei van het internet der dingen mogelijk maakt.

In dit kader wordt door sommige deskundigen gesproken van een internationale technologie-wedloop of zelfs van een nieuwe koude oorlog. Geopoliticoloog (hoogleraar politicologie aan New York University) Ian Bremmer spreekt van een koude oorlog over kunstmatige intelligentie[96], waarbij Europa de boot volgens hem overigens volledig gemist heeft. Anderen wijzen weer op het feit dat landen als Israël en de VS er standaard vanuit gaan dat er al aanvallers binnen zijn. In plaats van de ijdele hoop ze buiten te houden met de illusie van een digitale ophaalbrug jagen ze voortdurend op indringers.

Kader 13: Het European Centre for International Political Economy (ECIPE) waarschuwt Europa indringend voor digitale spionage, met name door (staatsgerelateerde hackers uit) China[97]. Dit zorgt voor een verzwakte concurrentiepositie, grote economische schade (circa 55 miljard euro per jaar) en baanverlies (mogelijk 289.000 banen). Door het Internet of Things, cloudopslag, 5G, en Industry 4.0 groeit de kans op digitale diefstal 'exponentieel' en Europa is juist relatief slecht beschermd. Dit terwijl de detecteerbaarheid en traceerbaarheid laag is, internationaal-juridische sanctiemogelijkheden beperkt zijn door staatsimmuniteit en doordat diplomatieke wegen doodlopen: landen als China en Rusland tekenen namelijk geen non-proliferatieverdragen.

De Chinese strategie is gericht op technologische werelddominantie en cyberspionage is daarbij een belangrijk middel. De VS en China zelf sluiten daarom delen van hun thuismarkt af, terwijl de Europese markt open is voor iedereen. Oftewel: zowel de voordeur als de achterdeur staat open. Dit heeft ook te maken met het feit dat Europa geen ICT-bedrijven als Cisco of Huawei heeft en daarom afhankelijk is van buitenlandse leveranciers. Daarom moet de Europese Unie volgens het European Centre for International Political Economy (ECIPE) de Chinese toegang tot de interne markt bemoeilijken. Door hogere veiligheidseisen aan producten te stellen, door technologie voor de overheid en in de vitale infrastructuur scherper te screenen en door sneller over te gaan op diplomatieke en economische sancties. Naast betere beveiliging van bedrijfsinformatie moet dit vooral zorgen voor druk op China om zijn agressieve gedrag te veranderen.

Feit is dat de toenemende spionage-dreiging samenvalt met protectionistische reflexen in het handelsbeleid van veel landen. Amerikaanse veiligheidsdiensten waarschuwen bijvoorbeeld voor het Chinese bedrijf ZTE. De financiële topvrouw van het Chinese Huawei werd op instigatie van de VS gearresteerd in Canada en landen als Australië, Duitsland, Frankrijk en het Verenigd Koninkrijk willen Huawei uit hun netwerken halen. Nederland moet (in EU-verband) zijn strategische positie bepalen. Alles zelf produceren is geen optie en het lukraak weren van buitenlandse bedrijven evenmin. Maar vooraf duidelijke eisen stellen aan buitenlandse leveranciers kan wel.

[96] https://www.nrc.nl/nieuws/2018/12/14/er-woedt-een-koude-oorlog-over-kunstmatige-intelligentie-a3060723
[97] Hosuk Lee-Makiyama (director of ECIPE): "Stealing Thunder (2018)

En op Europees niveau bepaalde sleuteltechnologieën in eigen hand houden kan ook. Hierbij kan gedacht worden aan kunstmatige intelligentie of bijvoorbeeld fotonica.

D66 stelt voor:

- Ontwikkel een Nationaal Technologie Kader om de staatsveiligheid te waarborgen. Dit bestaat allereerst uit een risicoanalyse gebaseerd op het bedrijf in kwestie, het land (regering en inlichtingendiensten) en de te importeren technologie zelf. Het tweede onderdeel is een objectief eisenpakket voor alle buitenlandse leveranciers die onderdelen van de vitale infrastructuur mogen leveren.
- Laat alleen leveranciers die volgens normen zijn getoetst, aan vitale sectoren leveren. Deze leveranciers moeten transparant zijn, auditrapporten toestaan en broncode-audits toelaten. Zorg voor voldoende capaciteit om dit te doen[98].
- Ontwikkel een Europese Technologie-Strategie in aanvulling op de nationale China-strategie en de nationale Rusland-strategie. Deze moet benoemen bij welke technologieën Europa niet afhankelijk mag zijn van buitenlandse spelers.
- Verbied in Europees verband de verkoop van hard- en softwareproducten die gaten in hun beveiliging hebben om veiligheidsdiensten ter wille te zijn. Op overtreding staan sancties, variërend van boetes tot uitsluiting van bepaalde markten.
- Laat ook bedrijven zich beter moeten wapenen, bijvoorbeeld door een vast percentage van de omzet te investeren in cybersecurity.
- Bescherm bedrijven die cruciaal zijn voor onze toekomstige concurrentiepositie (zoals ASML en NXP) in Europees tegen buitenlandse overnames. Hoewel marktbescherming op zichzelf geen goede strategie is, is dit wel nodig.

Cyberoorlog

Nadat de Militaire Inlichtingendienst (MIVD) begin oktober 2018 Russische hackers wist tegen te houden tijdens hun brutale cyberaanval op de OPCW, zei de Minister van Defensie dat Nederland in "cyberoorlog" was met Rusland. Dit riep in de Tweede Kamer de vraag op of deze daad dan ook viel onder artikel 5 van het NAVO-verdrag (en ook voor welke cyberactiviteiten van defensie dan een zogeheten artikel 100-brief nodig is[99]). Later

[98] Het niveau en de onafhankelijkheid van het Nationaal Bureau voor Beveiligingsverbinding (NBV) van de AIVD moet hierbij de norm zijn: https://www.aivd.nl/onderwerpen/informatiebeveiliging/het-nationaal-bureau-voor-verbindingsbeveiliging-nbv

[99] NAVO-artikel 5: een aanval op een NAVO-lid is een aanval op alle NAVO-leden. Artikel-100 brief: brief van de regering aan het parlement over de inzet van onze krijgsmacht voor de internationale rechtsorde.

nuanceerde de minister deze woorden, maar het maakte wel duidelijk dat er behoefte is aan een duidelijkere definitie en aanvullende internationale afspraken over digitale aanvallen.

Te meer omdat er door de toename van het aantal cyberaanvallen een soort digitaal Wilde Westen kan ontstaan: een situatie van feitelijke straffeloosheid. Het oorlogsrecht is weliswaar van toepassing maar lastig controleerbaar en handhaafbaar. Daarnaast is het vaak lastig te bepalen waar de aanval vandaan komt. Het is dus tijd voor nieuwe internationale regels voor praktijken die momenteel onvoldoende ondervangen worden onder bestaand internationaal recht. Met als doel het terugdringen van de grote hoeveelheden cyberaanvallen. Oftewel, een Haagse conventie tegen cyberaanvallen op vitale civiele infrastructuur, zoals elektriciteitsnetwerken, waterzuivering of ziekenhuizen.

D66 stelt voor:

- Zet via de VN in op een nadere digitale uitwerking van de Geneefse conventies[100], in lijn met de Tallinn manual 2.0 over internationaal recht in de cyber context.
- Zet via de EU in op internationale afspraken die gericht zijn op digitale non-proliferatie. Vergelijkbaar met het cybersecurityverdrag dat de VS en China in september 2015 met elkaar hebben gesloten.
- Stel een internationaal attributie-instituut in dat cyberaanvallen gaat onderzoeken om erachter te komen wie welke aanvallen heeft gelanceerd.
- Maak internationale afspraken om een KI-wapenwedloop met killer robots en onbemande drones te voorkomen. Maak ook afspraken over doelen die tijdens een cyberaanval gespaard dienen te blijven, zoals havens en energieleveranciers.

[100] Geneefse conventies zijn verdragen die de rechtsregels bepalen ten tijde van een gewapend conflict. Dit ter bescherming van gewonden, krijgsgevangenen en burgers in oorlogstijd.

Hoofdstuk 5. Politiek: van inzicht naar inzet

In de voorgaande vier hoofdstukken is uiteengezet hoe we digitalisering in goede banen kunnen leiden door digitale kansen beter te benutten, door te investeren in humane KI, door de datamacht van techreuzen te begrenzen en door aanvallen in de cyberstrijd alert af te slaan. Dit is een brede en gedeelde verantwoordelijkheid van burgers, maatschappelijke organisaties, bedrijven, wetenschappers en overheden.

De overheid strekt hierbij van de Europese Commissie tot aan lokale politici. Het is een taak van alle politici om digitale technologieën op voet te volgen en waar nodig besluiten te nemen om voordelen zoveel mogelijk te benutten en nadelen zoveel mogelijk te voorkomen. Hoewel veel digitale zaken een Europese aanpak vragen en sommige juist lokaal moeten worden opgevangen, spelen het kabinet en de Tweede Kamer een centrale rol bij het ontwikkelen van een goede digitale strategie voor Nederland. Los van elke inhoudelijke keuze die je hierbij kan maken, vergt dit een aantal procesmatige en organisatorische randvoorwaarden waaraan nu nog niet voldaan is.

Allereerst gaat het om voldoende kennis en expertise. Dit is niet alleen nodig om alle razendsnelle ontwikkelingen en grote hoeveelheden informatie te kunnen verwerken, maar ook om onafhankelijk van markten en lobbyisten te kunnen opereren. Deze kennis is deels een eigen verantwoordelijkheid, maar kan daarnaast ook op een collectief niveau worden georganiseerd door vaker hoorzittingen, debatten en werkbezoeken te organiseren. De interesse hierin is momenteel te laag en beperkt zich tot een te kleine groep ministers en Kamerleden. Hier moet verandering in komen. Bij de Algemene Politieke Beschouwingen van 2020 moet digitalisering het centrale thema zijn.

Kader 14: In 2017 bracht het Rathenau Instituut het rapport "Opwaarderen, Borgen van publieke waarden in een digitale samenleving" uit[101]. Daarin stelt zij dat de overheid, het bedrijfsleven en het maatschappelijk middenveld actie moeten ondernemen om publieke waarden in de digitale samenleving te borgen. Dit aan de hand van vijf concrete voorstellen.

Allereerst een interdepartementale werkgroep die toewerkt naar een kabinetsvisie op de omgang met de maatschappelijke en ethische betekenis van digitalisering, en die tevens zorgt voor politiek-bestuurlijke coördinatie. Ten tweede het versterken van de rol en positie van toezichthouders als de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt. Ten derde een zogenaamd "Digitaliseringsakkoord" dat de verantwoordelijkheden van bedrijven, overheid en

[101] Rathenau Instituut: 'Opwaarderen, Borgen van publieke waarden in een digitale samenleving' (2017). https://www.rathenau.nl/nl/digitale-samenleving/opwaarderen

maatschappelijke actoren omtrent de borging van publieke waarden in de digitale samenleving vastlegt. Te vierde een nationale dialoog over de betekenis van digitalisering voor de borging van publieke waarden. En als vijfde zorgen voor een periodieke politieke discussie in Eerste en Tweede Kamer over bestuurlijke oplossingen van maatschappelijke en ethische digitaliseringsvraagstukken[102].

Ten tweede moeten kabinet en Kamer als normsteller en regelgever zelf het goede voorbeeld geven op digitaal gebied. Het stimuleren of controleren van ontwikkelingen en het reguleren van bedrijven kan alleen door je eigen zaken op orde te hebben. Dat geldt niet alleen voor de uitvoering, zoals publieke dienstverlening en ICT-projecten van de overheid, het is ook principiëler van aard. Wie wil voorkomen dat algoritmes ongewenste besluiten nemen, moet zelf transparant zijn over het gebruik ervan. Wie de datamacht van techreuzen wil begrenzen, moet zelf terughoudend zijn met het verzamelen van persoonsgegevens. Wie cyberaanvallen wil voorkomen moet zelf gevonden softwarefouten zo snel mogelijk melden aan de maker zodat het gat gedicht kan worden. Een vorm van digitale zelfreflectie en discipline is dus nodig om het draagvlak voor politieke besluitvorming te vergroten.

Ten derde, moet de organisatie van het politieke debat verbeterd worden, net zoals het bestuur en de wetgeving rondom digitale veiligheid. Het debat komt nu namelijk maar moeizaam op gang. Dat het enige tijd kost voordat een relatief nieuw thema de politieke arena bereikt, is logisch. Echter, de toenemende aandacht van wetenschap en bedrijven maar ook maatschappij, media en mensen voor technologie en digitalisering is niet meer te ontkennen of te stoppen. Prioriteitlegging is niet extern afdwingbaar, terwijl ook meer kennis en tijd investeren een keuze is van partijen en politici zelf. Maar wat wel collectief kan en moet, is het verbeteren van de politieke behandeling van het thema digitalisering.

In hun recente uitgave “Digitalisering vraagt om doelgericht innoveren” doet het Rathenau Instituut vijf aanbevelingen voor een betere governance van de digitale transitie. De belangrijkste zijn een overkoepelende agenda voor digitalisering en inhoudelijke versterking –en waar nodig bundeling- van toezichthouders. Rathenau wijst bij beide op het belang van samenwerking en een Kamercommissie-overstijgende benadering.

De focus moet liggen op het wegnemen van versnippering als versperring voor een samenhangende aanpak van digitalisering: de digitale coördinatie moet beter. In de eerste plaats zijn er nu drie bewindspersonen voor digitale zaken: de Staatssecretaris van Economische Zaken (digitale economie), de Minister van Justitie en Veiligheid (digitale veiligheid), en de Staatssecretaris van Binnenlandse Zaken (digitale overheid). Op zich is dit beter dan het

[102] In 2018 publiceerde het Rathenau Instituut ”Digitalisering vraagt om doelgericht innoveren”. Te beschouwen als follow-up van “Opwaarderen”, waarin 5 aanbevelingen worden gedaan voor betere governance van digitalisering.

ooit geweest is, maar de snelle ontwikkelingen vragen meer stuurvermogen en daadkracht. Het volgende kabinet moet hier verandering in brengen. Ten tweede is er geen Kamercommissie die digitalisering in samenhang behandelt. Elke Kamercommissie behandelt zo nu en dan een digitaal onderwerp maar er is geen overzicht en geen overstijgende benadering. Aan deze politieke beleidsisolatie moet in 2019 verandering komen.

Ten slotte is er afgelopen decennia de nodige institutionele drukte rondom digitalisering ontstaan. Er zijn vele inspecties, toezichthouders, diensten, coördinatoren en adviesorganen, die zich met digitalisering bezig houden. Een greep: De Accountantsdienst Rijk (ADR), vier Rijksinspecties[103], het Bureau ICT Toetsing (BIT), De Autoriteit Persoonsgegevens (AP), de Autoriteit Consument en Markt (ACM), de Algemene Inlichtingen en Veiligheidsdienst (AIVD), De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Nationale Cybersecurity Centrum (NCSC), de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en de Cybersecurity Raad (CSR). Ook de drie non-parlementaire Hoge Colleges van Staat (de Raad van State, de Algemene Rekenkamer en de Ombudsman) houden zich in toenemende mate met digitalisering bezig. Dit is onvermijdelijk en niet per se problematisch, maar ook hier zou krachtenbundeling en coördinatie waarde hebben.

D66 stelt voor:

- Organiseer als politici en ambtenaren meer training in digitale vaardigheden. Denk aan kennis over digitale veiligheid bij gevoelige sectoren zoals transport, energie en het bankwezen. Stel naast het 'Bureau Onderzoek en Rijksuitgaven' (BOR) dat Kamerfracties ondersteunt op begrotingsgebied ook een 'Bureau Onderzoek en technologie' (BOT) in om fracties op technologie van informatie te voorzien.
- Geef als overheid het goede voorbeeld door kritischer naar jezelf te kijken. Zorg als overheid voor consistent en transparant beleid. Bij het uitbreiden van het internet der dingen (smart cities, zorg), bij het verzamelen en koppelen van data (surveillance, fraudebestrijding) en bij het gebruik van KI.
- Stel een Digitale Autoriteit in, direct onder minister-president[104], naar het voorbeeld van de *Government Chief Scientific Adviser* van het Verenigd Koninkrijk die het kabinet rechtstreeks adviseert over wetenschap en technologie. Deze bestrijkt de digitale overheid, de digitale economie, de digitale veiligheid en digitale ethiek.
- Alternatief: stel een minister voor Digitale Zaken in, vergelijkbaar met de Belgische situatie, waar de vicepremier verantwoordelijk is voor de digitale Agenda. Omdat Nederland meer een vakminister-cultuur dan een *chefsache*-cultuur heeft en omdat een coördinerend minister doorgaans weinig kan afdwingen, hebben we dit plan B.

[103] Inspectie van het Onderwijs, Inspectie Justitie en Veiligheid, Inspectie Sociale Zaken en Inspectie Gezondheidszorg en Jeugd (i.o.)
[104] In het Financieel Dagblad van 23 november 2017 pleitte D66-senator Alexander Rinnooy Kan in een opiniebijdrage ook al eens voor dit idee.

- Stel in aanloop naar deze Autoriteit of minister nog deze Kamerperiode een Vaste Kamercommissie Digitale Zaken in. Vergelijkbaar met de Vaste Kamercommissie Europese Zaken. Stel als presidium van de Tweede Kamer een onderzoek in naar de mogelijkheid van versnelde wetgevingstrajecten.

Bijlage 1: In te stellen organen

Een goede organisatie van digitalisering vraagt om sterke publieke organen. In deze visie doet D66 een aantal voorstellen voor het instellen van een orgaan. We zetten ze hier kort op een rij:

- Een internationaal attributie-instituut dat cyberaanvallen gaat onderzoeken om erachter te komen wie welke aanvallen heeft gelanceerd.
- Een Europese, niet politiek-gestuurde, toezichthouder die toegang krijgt onder de motorkap van digitale bedrijven en die sancties kan opleggen
- Een hoge Digitale Autoriteit, direct onder minister-president, naar het voorbeeld van de *Government Chief Scientific Adviser* van het Verenigd Koninkrijk die de premier en het kabinet rechtstreeks adviseert over wetenschap en technologie.
- Het alternatief is een minister voor Digitale Zaken, vergelijkbaar met de Belgische situatie, waar de vicepremier verantwoordelijk is voor de Digitale Agenda.
- Een algoritme-waakhond, die toezicht houdt op de inzet van algoritmes (en onderliggende datasets) door overheid en bedrijven met grote maatschappelijke impact en die de gevolgen voor mensen toetst en waar nodig corrigeert.
- Een Vaste Kamercommissie Digitale Zaken. Vergelijkbaar met de Vaste Kamercommissie Europese Zaken.

Bijlage 2: Begrippenlijst

- 2-factor-authenticatie: een authenticatie-methode waarbij je twee stappen correct moet doorlopen om toegang te krijgen tot het systeem of apparaat.
- 3D-printer: een printer die digitale informatie omzet in driedimensionale objecten.
- 5G: de vijfde generatie mobiel internet, nodig voor het internet der dingen. De opvolger van 4G.
- Algoritme: een reeks specifieke geprogrammeerde instructies die gebruikt worden om een probleem of te lossen of een taak uit te voeren.
- Big Data: zeer omvangrijke digitale datasets (die niet in een reguliere database te vatten zijn) waarvoor geldt dat de hoeveelheid, de snelheid en de variëteit alle drie zeer hoog zijn.
- Deep Learning: een vorm van machine learning die gebaseerd is op kunstmatige neurale netwerken. Door het menselijk brein na te bootsen wordt een zelflerend systeem gecreëerd. Dit gebeurt gelaagd, waarbij elke laag een onderdeel van het proces uitvoert.
- Drone: een onbemand vliegtuig, autonoom of op afstand bestuurd.
- Encryptie: versleuteling via een algoritme. End-to-end encryptie is een vorm van versleuteling die zorgt dat alleen verzender en ontvanger bij de informatie kunnen.
- Ethische hacker: een hacker die positief hackt om softwarefouten of beveiligingsrisico's aan het licht te brengen. Vaak in opdracht en altijd met als doel de vondst te rapporteren.
- Internet of Things (het internet der dingen): dit ontstaat door apparaten met het internet te verbinden, met als doel om steeds meer gegevens te kunnen uitwisselen.
- Kunstmatige Intelligentie: de intelligentie waarmee machines en software zelfstandig problemen oplossen. Het is tevens de wetenschap die zicht richt op het creëren van een kunstmatig verschijnsel met intelligentie. Algemene Kunstmatige Intelligentie is het vermogen alle taken te verrichten waar mensen toe in staat zijn, ook wel superintelligente KI genoemd.
- Machine Learning: de verzamelnaam voor het genre kunstmatige intelligentie waarbij computers steeds beter worden in het oplossen van problemen naarmate ze meer data ontvangen. Bij Reinforcement Learning gebeurt dit door te leren van fouten (trial and error), bij Supervised Learning op basis van gelabelde data, bij Unsupervised Learning juist met ongemarkeerde data die het slimme systeem zelf categoriseert.
- Netneutraliteit: het idee dat internetaanbieders (providers) open en vrije toegang moeten geven tot internetdiensten en deze dus niet verschillend mogen behandelen, mogen beperken, mogen beprijzen of mogen filteren.
- Netwerkeffect: het mechanisme dat maakt dat een product of dienst beter wordt en meer waarde krijgt naarmate het vaker gebruikt wordt.

- Neuraal netwerk: een groep verbonden zenuwcellen (of neuronen), zoals in de menselijke hersenen. Een kunstmatig neuraal netwerk is een computer systeem dat is gebaseerd op de werking van het biologische brein. Dit is de tegenhanger van de regel-gebaseerde systemen die de eerste fase van de kunstmatige intelligentie domineerden.
- Patch: een stukje software dat softwarefouten herstelt of software-updates uitvoert.
- Ransomware: kwaadaardige software (malware) die een computer blokkeert of die bestanden ontoegankelijk maakt.
- Robotica: computertoepassingen in het dagelijks leven (zoals robots of slimme, geautomatiseerde systemen).
- Singulariteit: het moment dat technologie intelligenter wordt dan de mens en zich onafhankelijk van de mens verder ontwikkelt. In de natuurkunde is dit het moment dat normale wetten niet meer gelden (zoals bij zwarte gaten).
- Zero-day exploit: een (nog niet geopenbaarde) softwarefout waar nog geen patch voor is en die derhalve gebruikt kan worden om te hacken.

Bijlage 3: Verantwoording, dankzegging en belangrijke bronnen

Deze Techvisie 2.0 is een update van onze eerste Techvisie uit 2016. Hiermee wil D66 een verdere bijdrage leveren aan het politieke debat over digitalisering. Voor de samenhang van dit verhaal hebben we de vele deelonderwerpen verdeeld over vier actuele hoofdthema's: digitale kansen, kunstmatige intelligentie, datamacht en cyberstrijd. Omdat deze vier elkaar onderling raken en alle maatschappelijke impact hebben, is hier geen hiërarchie in aangebracht. Als politieke partij richten we ons in deze visie hoofdzakelijk op de rol van de overheid om digitale technologieën in goede banen te leiden. Dat de overheid een cruciale rol te vervullen heeft, neemt niet weg dat burgers en bedrijven ook veel zelf kunnen doen om hun positie te versterken en kansen te benutten.

Deze Techvisie 2.0 is tot stand gekomen onder verantwoordelijkheid van de Tweede Kamerfractie van D66. Bij het ontwikkelen ervan hebben we gebruik gemaakt van een grote groep externe deskundigen. Deze hebben op verschillende manieren hun inbreng geleverd.

Allereerst vonden tussen 6 februari 2018 en 13 februari 2019 diverse rondetafelgesprekken en werkbezoeken plaats:

6 februari 2018 – Gesprek Cybersecurity (D66)
7 februari 2018 – Rondetafelgesprek Cybersecurity (Tweede Kamer)
24 mei 2018 – Rondetafelgesprek Internetbedrijven en Privacy (Tweede Kamer)
28 mei 2018 – Gesprek Kunstmatige Intelligentie (Microsoft/D66)
22 juni 2018 – Werkbezoek KI in de zorg (Philips Research/FME)
27 juni 2018 – Gesprek Vitale Infrastructuur (Vodafone-Ziggo/D66)
17 januari 2019 – Gesprek professor Virginia Eubanks (Tweede Kamer)
13 februari 2019 – Rondetafelgesprek ICT-projecten bij de overheid (Tweede Kamer)

Ten tweede hebben we circa dertig externe deskundigen gevraagd te reageren op een eerste versie. Ruim de helft hiervan heeft (ruimhartig) gebruik gemaakt van deze mogelijkheid.

Ten derde zijn in 2018 geregeld 1-op-1 gesprekken gevoerd met bedrijven, wetenschappers, brancheorganisaties, maatschappelijke organisaties en andere digitale deskundigen.

Dank aan de volgende mensen en organisaties

ACTI (Academy of Technology and Innovation)
AI4People
Annet Aris (Insead)
Christiaan Alberdink Thijm (Bureau Brandeis)
Jan Baan (Vanenburg Software)
Jaya Baloo (KPN)
Arie van Bellen (ECP)
Caspar van den Berg (Universiteit van Groningen)
Sjoerd Blüm (Royal Schiphol Group)
Machiel Bolhuis (Eneco Groep)
Frederik Zuiderveen Borgesius (IViR, Universiteit van Amsterdam)
Philip Brey (Universiteit Twente)
Dennis Broeders (Universiteit Leiden)
Lotte De Bruijn (Nederland ICT)
Stephen Deadman (Facebook)
Marieke Dekker (Liberty Global)
Ineke Dezentjé Hamming-Bluemink (FME)
Boris Dittrich (Human Rights Watch)
Michel van Eeten (TU Delft)
Dick van Egmond (Accenture)
Nico van Eijk (Universiteit van Amsterdam)
Arjan el Fassed (Google)
Iarla Flynn (Google)
Hans Folmer (Defensie Cyber Commando)
Jochem de Groot (Microsoft)
Wil van Gemert (Europol)
Anna Gerbrandy (Universiteit Utrecht)
Simon Hania (TomTom)
Wim Hafkamp (Rabobank)
Edo Haveman (Facebook)
Maaike Harbers (Hogeschool Rotterdam)
Koen Hindriks (Vrije Universiteit Amsterdam)

Jos Huigen (KPN)
Bart Jacobs (Radboud Universiteit)
Erik de Jong (FoxIT)
Erik Jonker (D66)
Frederik Kerling (Atos)
Leon Kester (TNO)
Alexander Klimburg (The Hague Centre for Strategic Studies)
Ad Krikke (DSM)
Ancilla van de Leest (Startpage.com)
Jeroen van der Meer (EY)
De Mr. Hans van Mierlo Stichting van D66
Catelijne Muller (EESC)
Geert Munnichs (Rathenau Instituut)
Thomas Myrup Kristensen (Facebook Europa)
Bart Pegge (Considerati)
Milan Petkovic (Philips Research)
Inge Philips-Bryan (Deloitte)
Theo van der Plas (Nationale politie)
Michiel Prinsen Geerlings (Vodafone-Ziggo)
Rina Joosten-Rabou (Seedlink)
Markus Reinisch (Facebook)
Alexander Rinooy Kan (D66)
Sabine Roeser (TU Delft)
Huibert van Rossum (Haven Rotterdam)
Jaap Schuler (EY)
Ieko Sevinga (Rabobank)
Marty Smits (SoSimple Solar)
Birgit Stein (EY)
Michiel Steltman (Stichting Digitale Infrastructuur Nederland)
Floor Terra (D66)
Wilbert Tomesen (Autoriteit Persoonsgegevens)
Kirsten Veldhuijzen (D66)
Rene Veldwijk (Ockham Groep)
Herna Verhagen (Cyber Security Raad)
Michael Vos (Microsoft)

Robert Went (WRR)
Willem Westerhof (ITsec)
Brenno de Winter (zelfstandig beveiligingsonderzoekers)
Patricia Zorko (Nationaal Cyber Security Centrum)

Veelgebruikte publicaties

De robot de baas, Wetenschappelijke Raad voor het Regeringsbeleid (2015)
De Wereld van Morgen, Richard van Hooijdonk (2017)
Homo Deus, Yuval Harari (2017)
LIFE 3.0, Max Tegmark (2017)
Ontzielde wereld, Franklin Foer (2017)
ON/OFF, Sidney Vollmer (2017)
The Essential AI Handbook for Leaders, Luka Crnkovic-Friis (2018)
The Future Computed, Microsoft (2018)
Responsible Development of AI, Google (2018)

Het Schrijfteam, 20 februari 2019,

Kees Verhoeven
Marijn van Vliet
Janne Gerritsen
Veerle Brink
Noortje Visser
Chris Mooiweer
Boaz Leupe