

Michel Rademaker, Plv. Directeur

Den Haag, 23-09-2019

Aan Tweede Kamer, Tijdelijke Commissie Digitale Toekomst (TCDT)

Betreft: Bijdrage Kennisbijeenkomst TCDT door Den Haag Centrum voor Strategische Studies

Hartelijk dank voor de uitgebreide gelegenheid die mij wordt geboden om bij te dragen aan deze kennisbijeenkomst ter voorbereiding van een parlementair onderzoek naar de mogelijkheden om de kennispositie op het gebied van digitalisering te versterken.

Verzocht is om bij te dragen aan een brede blik op het terrein van digitalisering en aan te kunnen geven op welke thema’s op het terrein van digitalisering door de Kamer aandacht zou moeten worden besteed!

HCSS is een denktank die haar analyses start vanuit de wereldwijde ontwikkelingen die steeds meer geopolitiek worden gekleurd. De focus van ons werk kleurt dan ook mijn bijdrage.

Ik heb mijn betoog ingericht langs de lijnen van internationale ontwikkelingen, voor de wereld, voor Europa en voor Nederland. Hierbij heb ik zowel een aantal bedreigingen als kansen benoemd. Ik ben me daarbij tevens bewust dat ik geen compleet heb kunnen schetsen.

Gegeven het karakter van deze bijeenkomst hoop ik dat de onderstaande vragen deels worden gevoed door in dit stuk.

1. Thematische Agenda: Wat moet de kamer weten?
2. Maatschappelijk en Politiek afwegingskader: Welke vragen zou de Kamer moeten stellen?
3. Institutioneel: Hoe kan de Kamer in staat zijn om tijdig op de hoogte te zijn en eventueel bij te kunnen sturen?

**Ontwikkelingen**

De ICT-participatie (burgers en bedrijven) in de wereld neemt nog steeds toe. Hierdoor ontstaan kansen voor iedereen. De westerse wereld is nog steeds koploper in gebruik, Nederland voert dat mede aan. Onze ICT-infrastructuur, het individueel gebruik, de publieke diensten, het zakelijk gebruik en wet- en regelgeving zijn ‘on par’. Hiermee is de ICT-sector een relevante economische speler in Nederland. En voorwaardenscheppend voor feitelijk alle andere sectoren. De sector kan daarmee niet worden onderschat. We scheppen daarmee (economische) kansen, inclusiviteit en we zijn een voorbeeld voor veel andere landen maar de technologie introduceert ook kwetsbaarheden. De snelle technologische en geopolitieke ontwikkelingen dwingen ons om niet stil te zitten maar steeds proactief vooruit te kijken en te investeren.



Figuur GFCE Cyber monitor, ontwikkeld door HCSS

Bij Kunstmatige Intelligentie (AI)-investeringen loopt de EU en Nederland achter bij rest van de wereld. Er zijn wel plannen hier snel verandering in aan te brengen. Vanaf 2021 voorziet de EU een jaarlijkse investering van zo’n 20 Miljard euro. Ook Nederland is bezig. Binnenkort komt het Strategisch ActiePlan AI (SAPAI) uit en op 8 oktober wordt dit in Den Haag gelanceerd evenals het beoogde hoofdkwartier van CLAIRE, de Confederation of AI Laboratories in Europe. De hoop is dat de opgelopen achterstand met Amerika en China hiermee enigszins wordt ingelopen. Nederland met de stad Den Haag als voorvechter van Vrede en Recht (dit is opgenomen in onze grondwet) ook in de gedigitaliseerde wereld, heeft hierbij een perfect profiel. Normatieve AI is een onderwerp dat tot een belangrijk onderdeel van de Europese AI-strategie is uitgeroepen. Dat is ook een onderscheidende rol die Nederland zich kan aanmeten. Daarnaast is accountability is een belangrijk opkomend thema dat raakt aan alle ICT-ontwikkelingen van Fake News tot de nieuwste AI-technologie. De eerste principes rond accountability zijn ontwikkeld en moeten nu worden vertaald en ondersteund door instrumenten en tools. Op 6 & 7 november is de tweede Summit on Accountability in the Digital Age in het Vredepaleis waar dit besproken gaat worden.

***Bedreigingen***

Westerse waarden nemen in de wereld aan invloed af door de opkomst van autoritaire regimes met grote economische macht, andere waarden en afwijkende principes. Westerse ethiek en normen voor verantwoordelijk gedrag staan daardoor onder druk.

We zien dat met de ontwikkelingen/versnippering van het Internet, onderdelen door regeringen binnenlands volledig worden gecontroleerd door de staat zoals in China maar ook Rusland....

Met de economische en geopolitieke opkomst van China, o.a. via hun One Belt One Road of Nieuwe Zijderoute initiatief ontstaat er een nieuwe dynamiek die al een tijdje aan de gang is. Dit levert enorm veel politieke invloed die wordt gecombineerd met economische marktpotentie maar ook de mogelijkheden voor het genereren en verzamelen van veel data, op een wijze die de EU niet voorstaat. Data zijn erg belangrijke voedingsstoffen voor Kunstmatige Intelligentie (AI), 5G-netwerken zijn erg belangrijk voor snelle verbindingen en grote volumes aan datatransport. En met het Internet of Things (IoT) wordt een steeds nauwere verbinding met eindgebruikers/klanten en apparaten gecreëerd en dat genereert ook weer enorme hoeveelheden bruikbare data.

Als een land vooroploopt met AI, 5G, IoT creëert het daarmee het potentieel voor de ontwikkeling van de nieuwe industriële standaarden en daarmee het vermogen om de volgende economische grootmacht te worden zoals het Verenigd Koninkrijk met stoommachine en Amerika de ICT-revolutie heeft doorlopen. Dit heeft tevens de potentie de economische veiligheid van Europa en Nederland te ondermijnen in geval hier misbruik van wordt gemaakt. De NCTV heeft dit in 2018 ook onderkend door een onderzoek naar de economische veiligheid.

“Nederland is gebaat bij een open en vrijemarkteconomie. Daar horen overnames en investeringen van Nederland in het buitenland bij, maar ook overnames en investeringen van buitenlandse partijen in Nederland. Daarnaast is de inkoop en aanbesteding van buitenlandse producten en diensten niet meer weg te denken uit onze economie. Echter, bedrijven kunnen naast economische motieven ook andere motieven hebben. Zij kunnen bijvoorbeeld, openlijk of verborgen, gestuurd worden door een staat. Via het bedrijf kan dan de geopolitieke invloed vergroot worden van een land door het verwerven van informatie, geld, middelen en grondstoffen. Met deze economische machtsmiddelen kunnen andere landen onder druk worden gezet of kan de handelingsvrijheid van landen worden beperkt en kunnen er risico’s voor de nationale veiligheid ontstaan.”[[1]](#footnote-2)

We zien ook dat een toenemend aantal nationale veiligheidsbeoordelingen cybersecurity heeft geïdentificeerd als de belangrijkste of een van de belangrijkste dreigingen voor de nationale veiligheid. Het groeiende inzicht is dat spanningen tussen staten escaleren in cyberspace. Dit is vooral te danken aan de toenemende inzet van statelijke of aan de staat gelieerde cyberoperaties voor nationale doeleinden. De DDoS aanval in 2007 op Estland, een van de meest gedigitaliseerde landen, waarbij overheidsinstellingen, media, en financiële instellingen werden platgelegd, vormende een nieuwe vorm van conflict in cyberspace waarbij statelijke aanvallen worden ingezet door proxy actoren ter bevordering van het buitenlandbeleid. Daarbij houdt de statelijke aanvaller enige mate van *plausible deniability*. Daarna volgde een reeks andere strategische cyberaanvallen die de krantenkoppen hebben gehaald, zoals die in Georgië in 2008, Stuxnet in 2011, Sony Pictures in 2014, het Franse mediahuis Tele5, een Duitse staalmolen en het elektriciteitsnet van Ukraine in 2015. Recentelijk zagen we een golf van ransomware aanvallen zoals WannaCry en NotPetya (2017), en een disinformatiecampagne die zich richtte op het beïnvloeden van Amerikaanse en Europese verkiezingen.

Conflicten tussen staten nemen nieuwe vormen aan en cyberoperaties spelen een steeds belangrijkere rol. Deze operaties beogen inbreuk te maken op de beschikbaarheid en integriteit van gegevens- en ICT-systemen via wat kan worden omschreven als een computernetwerkaanval (Computer Network Attacks). Dit kan worden bereikt door denial of service of destructieve invoeging van malware en andere middelen. Het vereist vaak evengoed spionage of inlichtingenactiviteit - dat wil zeggen het vermogen om de vertrouwelijkheid van gegevens aan te tasten. Deze voorloper, voorheen bekend als Computer Netwerk Exploitation, bevat functies die bekend staan als inlichtingen, cyberspionage, surveillance en verkenning en operationele voorbereiding van het de omgeving (voorbereiding voor een aanval). Inderdaad, de vermogens van staten om kinetische schade toe te brengen in cyberspace vereist in verschillende mate het vermogen om inlichtingenoperaties uit te voeren. De exacte aard van deze aanvallen is echter vaak onduidelijk. Terwijl sommige cybercapaciteiten zijn gereserveerd voor het slagveld en tenminste enigszins gedefinieerd zijn, zijn andere mogelijkheden minder duidelijk. Het gebrek aan duidelijkheid over de offensieve cybercapaciteiten, betekent dat het erg moeilijk is om volledig te beschrijven wat de "middelen" (bezorgsystemen of wapens) zijn. Cyberspace biedt staten een sluier van anonimiteit om kwaadwillende cyberactiviteiten te ondernemen om strategische en operationele voordelen te behalen. Recentelijk weten we dat staten meer openlijk betrokken zijn bij cyberaanvallen, waaronder verschillende vormen van Computer Network Attacks, cyberspionage, en desinformatiecampagnes. Terwijl attributie nog steeds moeilijk is, zien we ook dat staten die aanvallen doorstaan of onderscheppen steeds vaker hun aanvaller weten te attribueren.

Dit geeft aan dat cyberaanvallen het nieuwe normaal worden en daarom aansluiten bij de al zeer geladen nieuwe realiteit van schijnbaar alomtegenwoordige cyberspionage. Hierachter schuilt de bezorgdheid dat een catastrofale confrontatie in cyberspace tussen staten zou kunnen plaatsvinden. Hoewel dit vooruitzicht gedeeltelijk verband houden met de huidige geopolitieke spanningen, bestaat er een aanzienlijke en brede bezorgdheid dat het vermogen van overheden om de dreiging van een groot conflict in cyberspace te beheersen, wordt belemmerd door de complexiteit van attributie, de dominante rol van niet-statelijke actoren (aanvaller, slachtoffer, media of drager van aanvallen), evenals de onduidelijke relaties die deze actoren hebben met de overheid. En tenslotte de snelle ontwikkeling van de technologie zelf, zorgt voor potentieel onverwachte toekomstige schokken die aanzienlijke gevolgen hebben voor de nationale veiligheid.

**Gerapporteerde cyberspionage**



**Disinformation**



**Strategische Cyber aanvallen (dus met een geopolitieke component)**



***Internationale ontwikkelingen en Nederlandse Kansen***

Pogingen om deze ondermijnende en disruptieve activiteiten op intergouvernementeel niveau aan te pakken kennen verschillende mate van succes. In 2013 heeft de VN Group of Governmental Experts (GGE) in het ICT-gebied, het belangrijkste voertuig binnen de Eerste Comité van de VN dat zich bezighoudt met internationale veiligheid en ontwapening, verklaard dat het internationale recht van toepassing is en essentieel is voor het handhaven van vrede en stabiliteit en het bevorderen van een open, veilig, vreedzaam en toegankelijke ICT-omgeving. Echter is het soms nog onduidelijk wanneer, en meer specifiek, hoe het bestaande internationale recht moet worden geïnterpreteerd en toegepast in dit nieuwe domein. Daarnaast laten recentelijke gebeurtenissen en aanvallen een zorgwekkende trend zien waarbij zowel statelijke als niet-statelijke actoren gedrag vertonen dat de stabiliteit van cyberspace bedreigt, deels door het bestaan van deze ‘juridische grijze gebieden’.

Het vaststellen van nauwkeurig afgebakende wettelijke verantwoordelijkheden voor de verschillende regimes in cyberspace is vaak niet mogelijk. Juridisch bindende overeenkomsten zijn vaak te moeilijk en te tijdrovend gezien de definitieve en ideologische verschillen tussen Oost en West. De westelijke cybersecurity benadering richt zich met name op de technische veiligheid van de vertrouwelijkheid, integriteit en beschikbaarheid van data en de systemen, terwijl de Oostelijke benadering niet zozeer gaat om de status van de data, maar waarvoor die gebruikt wordt. Voorbeelden zoals de Great Chinese Firewall en gelijksoortige Russische voorstellen, tonen aan dat autocratische landen dit middel vooral inzetten om dissidente en kritische inhoud offline te halen – teneinde hun regime veilig te stellen. Terwijl landen als Rusland en China heel graag een intergouvernementeel internet willen, hebben westerse democratieën zich geëngageerd tot een niet-statelijk internet, en terecht. Dit betekent niet dat elke betrekking van de overheid daarmee ongewenst is. Wetgeving die overheden en bedrijven aansprakelijk stellen en de burger zijn privacy en veiligheid bevorderen zijn van belang. In het grotere geheel moeten overheden voorzichtig omgaan met hun invloed en niet impliceren dat het Internet een staatsgebouw is. Net als de *high seas* is het van iedereen.

Daarom richtte de internationale westerse gemeenschap zich vooral op het ontwikkelen van vrijwillige, juridisch niet-bindende overeenkomsten – namelijk gemeenschappelijke normen van aanvaardbaar gedrag. Deze normen geven een versterkte interpretatie van het bestaand internationaal recht en juridische overeenkomsten in plaats van te proberen om nieuwe wetgeving te creëren. Hoewel de GGE-rapporten van 2013 en 2015 belangrijke stappen zijn om multilaterale consensus te scheppen, zien we dat hedendaagse geopolitieke opvattingen steeds verder van elkaar wegdrijven. Deze multilaterale stagnatie werd zichtbaar wanneer de vorige GGE in 2017 er niet in slaagde om consensus te bereiken. Het Eerste Comité van de VN is nu verdeeld in twee concurrerende processen: een Open-Ended Working Group (Russisch voorstel) en een GGE (geleid door de VS).

Ondanks hun traditionele dominantie over alle vragen met betrekking tot internationale vrede en veiligheid, vormen overheden slechts een van de drie actorgroepen in het cyberspace ecosysteem. Het Internet wordt bestuurd door een complex ecosysteem van stakeholders, elk met haar eigen set regels, normen, standaarden en processen. Het vermogen van de private sector, die de meeste digitale en fysieke systemen, producten en diensten in cyberspace bezit, en het maatschappelijk middenveld, dat grotendeels verantwoordelijk is voor het coderen en uitvoeren van de meest elementaire Internetfuncties, om gelijksoortige normen te creëren is daarom van groot belang. Overheden alleen kunnen niet beslissen over alle aspecten van cyberspace - in plaats daarvan is hun vermogen om eigen normen op te stellen grotendeels afhankelijk van de normen die anderen al hebben vastgesteld. Gezien dit complexe landschap is het onwaarschijnlijk dat er een enkelvoudige juridische oplossing bestaat die zowel afdwingbaar als inclusief is. In plaats van meer verdragen, is de oplossing deels al meer dan 400 jaar bekend bij veel Nederlanders - vrede en winst vereisen algemeen aanvaarde principes. Sinds Hugo Grotius zijn "mare liberum" formuleerde, is het Nederlandse beleid zich terdege bewust van het belang om internationaal gedefinieerde gedragsregels vast te stellen. In technische termen betekent dit het ondersteunen van de open standaarden die ten grondslag liggen aan Internet. Maar op politiek niveau betekent dit dat we ons moeten inzetten voor een proces van internationale en niet-statelijke normvorming die regels voor iedereen biedt.

Een van de uitdagingen om overeenstemming te bereiken over gedragsnormen in cyberspace is dat normen - en de bijbehorende praktische implementatiemaatregelen, zoals *Confidence Building Measures* (CBM's) - soms worden geformuleerd door een bepaalde groep actoren, maar naar verwachting worden uitgevoerd door een andere. Dit vereist dat de actorgroepen, regimes en initiatieven elkaars mandaat of legitimiteit volledig erkennen. Dit is niet automatisch het geval. Overheidsactoren kunnen worstelen met het accepteren van de legitimiteit van individuele ingenieurs die het Internet grotendeels in hun vrije tijd bouwen, terwijl dezelfde niet-statelijke actoren vaak de kennis, intentie of capaciteiten van de overheid minachten.

Werken in het gehele cyberspace ecosysteem is daarom vooral een kwestie van het accepteren van wederzijdse legitimiteit. Elke norm, elk project of elk initiatief dat een echt wereldwijd bereik en effect op cyberspace wil hebben, moet om te slagen de steun hebben van belangrijke actoren in het gehele regimecomplex. Deze actoren worden als legitiem beschouwd vanwege hun vermogen om representatief te zijn voor hun kiezers (leden, burgers of klanten), op de hoogte te zijn van de technische details binnen hun vakgebied, of vanwege het vermogen om veranderingen praktisch te bewerkstelligen. Het accepteren van een van deze definities van legitimiteit is gelijk aan het vertrouwen in het oordeel van deze actoren om op zijn minst relevant te zijn in het bredere discours. Vertrouwen tussen deze verschillende statelijke en niet- statelijke actoren is de sleutel tot cyberstabiliteit

Het is om deze reden, dat de Global Commission on the Stability of Cyberspace werd geïnitieerd door het *Den Haag* Centrum van Strategische Studies (HCSS) met de steun van het Nederlandse Ministerie van Buitenlandse Zaken en tal van andere partners zoals Microsoft, Internet Society, Afilias, de overheid van Frankrijk en Singapore, etc. De commissie betrekt de relevant stakeholders bij het ontwikkelen van normen en beleid die de internationale veiligheid en stabiliteit verbeteren. Dit Nederlands initiatief slaagt erin de wereldwijde discussie over verantwoord gedrag in cyberspace te hervormen en heeft normen gecreëerd voor ongekende internationale problemen. Het identificeert of eventueel aanvullende formats of initiatieven nodig zijn om de vastgelopen discussies te bevorderen - tussen het Oosten en het Westen, maar ook tussen overheden en niet-statelijke actoren. De commissie heeft tot nu toe al vooruitgang geboekt - de norm ter bescherming van de publieke kern van Internet is nu EU-wetgeving d.m.v. de EU Cybersecurity Act, en de Paris Call for Trust and Security in Cyberspace, een verklaring van 547 gelijkgestemde staten, bedrijven en maatschappelijke organisaties, onderschrijft 5 van de 8 GCSC-normen. Initiatieven zoals deze, het Global Forum on Cyber Expertise, het Universiteit Leiden Cyber Norms Programma, en anderen tonen aan dat publiek-private samenwerking van Nederlandse bodem een internationaal bereik heeft en Den Haag op de kaart zet als stad van Vrede en Recht in de gedigitaliseerde wereld.

**AI-Technologie**

AI-technologie roept momenteel veel vragen op. De technologie verontrust gebruikers en bedrijven soms waardoor de ontwikkeling en het gebruikt daarvan terughoudend is. Dit wordt gevoed door excessen van bekende internationale corporates die dataverzamelingen met behulp van AI manipuleren en (her)gebruiken zonder toestemming maar ook door het idee dat AI zichzelf ongecontroleerd kan door ontwikkelen zonder dat mensen zicht hebben op de consequenties.

Dit draagt niet bij aan het vertrouwen en de ook in EU verband gestelde ambities dat AI-technologie samenhangt met de notie dat respect moet worden betoond aan menselijke autonomie, het voorkomen van schade (*do no harm), fairness* en *explainability*.

Nederland heeft in het afgelopen decennium internationaal erkenning gekregen voor haar maatschappelijk verantwoorde benadering van innovatie en nieuwe technologie: Maatschappelijk Verantwoord Innoveren (MVI), zoals uitgewerkt in een 12 jaar lopend NWO- programma (2007-2019). Deze Nederlandse aanpak van innovaties met maatschappelijk grote impact heeft navolging gekregen in de EU via het R&D-programma Horizon2020 (2010-2020) van de Europese Commissie onder de naam Responsible Research and Innovation (RRI). Ook buiten Europa, in VS en China, kreeg het idee van Responsible Innovation bekendheid en navolging. Vanaf 2020 zal NWO in Nederland in samenwerking met een aantal ministeries de MVI-benadering verder gestalte geven in onderzoek naar verantwoorde digitale innovaties. Een community van circa 100 personen, bestaande uit onderzoekers van kennisinstellingen, beleidsadviseurs van overheid en experts uit het bedrijfsleven zullen gezamenlijk digitale oplossingen (waarbij een belangrijke rol van AI is weggelegd) voor maatschappelijke vraagstukken ontwerpen, die aan publieke waarden zoals accountability, transparantie, privacy en veiligheid voldoen.

De VN en een aantal Internationale Organisaties (e.g. OECD, UNESCO) hebben recentelijk erkend dat innovatieve technologie en wetenschap nu dringend nodig zijn in aanvulling op recht, economie, internationale betrekkingen en, diplomatie om tot duurzame oplossingen te komen voor de grote problemen van de wereld, zoals neergelegd in de UN SDGs. AI en Data Science nemen daarbij ontegenzeggelijk een zeer bijzondere plaats in. Zij kunnen inzicht bieden – mits verantwoord ontwikkeld en gebruikt - in een complexe en dynamische wereld en daarmee de basis leggen voor beter beleid en verantwoorde beslissingen.

Nederland en Den Haag hebben zich reeds een bijzondere positie verworven op dit gebied van AI for Humanity, zoals Macron en Brussel de EU-strategie betitelen. Nederland en Den Haag mogen zich op dit gebied op internationale belangstelling verheugen. Zo onderneemt Nederland hoogwaardige activiteiten op het gebied van AI & GovTech, AI & Law, RegTech, CivicTech, AI and Humanitarian Aid, International humanitarian law and Autonomous Weapons, AI for global development, AI and Human Rights. Het ligt in de rede AI-toepassingen in het domein van conflict studies, Peace Tech, Justice Tech, Global Governance, Human Security, Cybersecurity, Counter Terrorism, rule of law en, access to justice verder te ontwikkelen en kennis en onderzoek verder te stimuleren.

De inhoudelijke uitdagingen zijn formidabel: Vragen over de global governance van AI, de gedeelde verantwoordelijkheid van statelijke actoren voor toepassingen van AI, het gebruik van AI om mondiale vraagstukken op te lossen zonder daarbij mensenrechten te schenden etc. Nederland kan zich op deze terreinen internationaal onderscheiden, nieuwe kennis genereren en nieuwe diensten en producten ontwikkelen, maar ook een plaats zijn waar AI-toptalent zich met de vraagstukken van de wereld van morgen bezighoudt.

Dit vraagstuk vraagt om focus op:

**Human Capital ontwikkeling**

Er is meer kennis en talent nodig voor de moreel en juridische verantwoorde toepassing van nieuwe technologieën.

**Innovatie & Onderzoek**

Nederland heeft een voorbeeldfunctie op het gebied van verantwoorde innovatie. Er is een start gemaakt met een met NWO- programma gericht op fundamenteel onderzoek.

Nederland heeft een voorbeeldfunctie op het gebied van verantwoorde innovatie. Er is een start gemaakt met een met NWO- programma gericht op fundamenteel onderzoek.

Een Nationaal Kenniscentrum voor Verantwoorde AI-toepassing zou kunnen worden opgezet, waar kennis en methoden worden ontwikkeld die nodig zijn voor de maatschappelijk verantwoorde toepassing van AI.

**Ecosysteembenadering**

Om op nationaal niveau te bewaken dat de samenwerking goed gecoördineerd en verantwoord wordt opgezet en uitgevoerd is er mogelijk behoefte aan zoiets als een Nationale AI Raad waarin Kennisinstellingen, Overheden, Bedrijfsleven en Onderwijsinstellingen in gezamenlijkheid (naar analogie van de nationale cybersecurityraad) bijeenkomen en adviezen opstellen.

**Bewustwording**

Binnen Nederlandse maatschappij is in vele lagen weinig acceptatie voor toepassing en ontwikkeling van AI. Terwijl AI in veel gevallen een positieve bijdrage levert aan de maatschappij, zoals op het gebied van voedselverspilling, optimalisatie van logistiek en veiligheid. Het is noodzakelijk helder te maken wat AI kan betekenen voor de maatschappij, mist goed ingezet.

**Wet & regelgeving**

Er moet passende wet & regelgeving worden ontwikkeld voor deze nieuwe technologische ontwikkeling, inclusief certificering en keurmerken.

**Vergroten capaciteit opleidingen**

Het opleiden van goed geschoold, en voldoende talent is van cruciaal belang voor de commercialisering van elke opkomende technologie. De gemiddelde leeftijd van de ingenieurs die verantwoordelijk waren voor het Amerikaanse Apollo programma ten tijde van de eerste maanlanding was 28 jaar. Voor AI zal dan niet anders zijn: de groeiende vraag naar talent op het gebied van Artificial Intelligence en Data Science zal grotendeels vervuld worden door jong talent dat uitstroomt van de opleidingen aan onze universiteiten en hogescholen.

Het aanbod aan universiteiten is kwalitatief hoogwaardig, maar er zijn onvoldoende docenten. Daarom hebben de meeste computerkunde opleidingen in Nederland in 2018 een numerus fixus ingesteld. Het aantal AI-studenten schijnt ironisch genoeg gedaald in Nederland. Wat betreft de hogescholen is het aanbod nog onvoldoende als het om Artificial Intelligence en Data Science gaat.

Met het schetsen van deze situatie heb ik geprobeerd duidelijk te maken dat Nederland een toekomstgerichte strategische positionering en programmering moet nastreven. Een die gericht is op de grote systeemtransities die de komende twee decennia voor enorme invloed zijn op hoe onze waarden zich gaan vertalen in het digitale domein, hoe we. Ons geld gaan verdienen en de wijze waarop we als maatschappij, overheid en burgers samen optrekken en welvarend blijven.

1. <https://www.nctv.nl/organisatie/nationale_veiligheid/programma_economische_veiligheid/index.aspx> [↑](#footnote-ref-2)