

Kansen en bedreigingen van nieuwe technologieën voor onze digitale economie

In het regeerakkoord is aangekondigd dat Nederland gaat investeren in sleuteltechnieken en innovaties gekoppeld aan maatschappelijke thema's, zoals Quantum Computing, Artificial Intelligence (AI) en Cyber Security. Hiermee wil Nederland een van de leidende spelers op het gebied van Quantum blijven* en blijven op het gebied van AI. En op gebied van cyber security wordt bijvoorbeeld gewerkt aan de introductie van betaalbare data diodes op de (inter)nationale markt. Dit alles met het oog op het oplossen van maatschappelijke uitdagingen, de economische kansen en het verdienvermogen van Nederland in de toekomst.**

Ook op de One Conference – die van 1-3 oktober plaatsvindt in Den Haag en wordt georganiseerd door het ministerie van EZK en het Nationaal Cyber Security Centre (NCSC-NL) van het ministerie van J&V- is er aandacht voor deze onderwerpen. Er wordt gesproken over de relatie van deze nieuwe technologieën tot onze digitale veiligheid en privacy. Want wat gebeurt er als encryptiecodes gekraakt kunnen worden door de Quantum Computer, hoe kunnen we nu al anticiperen op deze risico's en hoe benutten we AI voor de beveiliging van bijvoorbeeld onze water- en elektriciteitsvoorzieningen?

Om de risico's en kansen van nieuwe technologieën in relatie tot cyber security in kaart te brengen heeft het nationale veiligheidscluster HSD in samenwerking met verschillende partijen drie duidingsstudies gedaan. Joris den Bruinen, directeur HSD: "Hieruit komt een aantal kansen die we met elkaar – bedrijven, overheden en kennisinstellingen - kunnen en ook moeten pakken om de positie van Nederland te behouden. Hierbij is de uitdaging om een balans te zoeken tussen wat er technisch allemaal mogelijk is en wat we ethisch en juridisch wenselijk vinden. Het betrekken van de eindgebruikers en maatschappij is hiervoor van belang."

Automated cyber security

Een aantal van de bovengenoemde kansen wordt uitgewerkt tot concrete programma's binnen het automated cyber security consortium. Dit is een publiek private samenwerking tussen TNO, een aantal bedrijven, de Provincie Zuid-Holland en HSD Office gericht op betrouwbare data en de continuïteit van ICT-netwerken en -systemen over de verschillende toepassingsgebieden heen. Noura El Ouajdi van TNO: "Gerichte en effectieve cyber security vergt een integrale aanpak en cross-sectorale kennis en ervaring. Aanvullend onderzoek op het gebied van AI alsmede de doorvertaling naar praktische oplossingen is van groot belang om snel, effectief en adequaat te kunnen handelen op het moment dat een cyber security incident zich voordoet."

Quantum Internet

Een andere kans is het beschikbaar stellen van quantum internet aan bedrijven, zodat zij met deze techniek kunnen innoveren op gebied van cyber security. Professor Stephanie Wehner, QuTech: "Een quantum internet werkt met quantum bits, zogenaamde qubits. Qubits gedragen zich volgens de regels van de quantummechanica. Qubits kunnen niet gekopieerd worden zonder verstoord te worden. Dit maakt een quantum internet heel veilig, maar vormt tegelijkertijd een probleem voor de communicatie over grotere afstanden, omdat het onmogelijk is om het signaal te versterken of te herhalen.

In het voorjaar van 2019 hebben Nederlandse kennisinstellingen en bedrijven in kaart gebracht wat er allemaal moet gebeuren om hun ambitie ten aanzien van quantumtechnologie waar te maken. [Deze nationale agenda](#) vormt het startpunt en beoogt een vliegwiel in gang te zetten. Door al

in een vroeg stadium te investeren in de ontwikkeling van quantumtechnologie kan Nederland internationaal een sterke positie verwerven.”

Open Source Data Diode

Nederland blinkt uit als het om Data Diodes gaat. Deze data diodes worden verkocht in het buitenland en hierin streven we andere landen voorbij. Het is een device (hardware & software) dat dataverkeer in slechts één richting mogelijk maakt. Zo kunnen data diodes netwerken en systemen beschermen tegen externe cyberdreigingen. Omdat ze relatief kostbaar zijn, worden ze tot nu toe alleen ingezet voor bijvoorbeeld de bescherming van onze vitale infrastructuur en staatsgeheime dossiers. Defensie heeft in samenwerking met HSD Office gekeken of er een betaalbare open source Data Diode ontwikkeld kan worden. Zodat ook bedrijven en zelfs mensen thuis hier gebruik van zouden kunnen gaan maken om bijvoorbeeld hun aan internet verbonden systemen en gadgets mee te beveiligen. Inmiddels is een ‘demonstrator’ in de maak.

“Met deze concrete programma’s, die we vanuit HSD Office in samenwerking met vele partijen aanjagen, initiëren en faciliteren, leveren we met elkaar een bijdrage aan de concrete uitvoering van het missiegedrevenbeleid van de rijksoverheid en de kennis & uitvoerings-/actieagenda’s op de gebieden van Quantum Computing en AI”, aldus Joris den Bruinen.

*<https://www.innovationquarter.nl/robert-dijkgraaf-overhandigt-nationale-agenda-quantumtechnologie-aan-mona-keijzer/>

**<https://dutchdigitaldelta.nl/nieuws/nederlandse-strategie-op-ai-gebied>