DOOR MARTIJN DEKKER

Quantumtechnologie: impact verzekerd

Opkomst van technologie geeft altijd aanleiding tot nieuwe mogelijkheden, businessmodellen en toepassingen. We hebben dit gezien bij de opkomst van computers, van het Internet en van de mobiele telefoons. Sommige van deze toepassingen van technologische ontwikkelingen zijn vrij voorspelbaar, en anderen verrasten bestaande bedrijven en hun leiders. Een bekend voorbeeld van dat laatste is de opkomst van de iPhone, die door leiders van Microsoft werd afgedaan als een onzinnig apparaat omdat het geen fysiek toetsenbord heeft. De stormachtige ontwikkeling van de smartphone die volgde liet zien hoe mis zij het hadden.

Quantumtechnologie is al decennia in ontwikkeling. Ook van deze technologie is soms gezegd dat het tot niets leidt of dat het een theoretisch toekomstbeeld is. Toch lijkt nu een kantelpunt bereikt en is deze technologie zich nu snel aan het ontwikkelen met reële implementatiemogelijkheden in de komende 5 tot 10 jaar. Die ontwikkelingen zullen grote impact hebben op onze samenleving en economie. Voor we ingaan op wat de gevolgen van het ontwikkelen van deze technologie zijn, zullen we eerst uitleggen over welke technologie we het hebben.

Als mensen denken aan quantumtechnologie, denken zij vaak aan een quantumcomputer. Een quantumcomputer is een machine die algoritmes uit kan voeren door manipulaties van zogenaamde *qubits*. Qubits zijn fysieke schakelingen die niet 'aan' of 'uit' zijn (zoals in een klassieke computer) maar die meerdere toestanden tegelijkertijd kunnen hebben. Deze superpositie van toestanden is een quantum-mechanisch fenomeen dat al bijna 100 jaar bestudeerd wordt door wetenschappers. Algoritmes die dit gebruiken blijken soms veel efficiënter te zijn dan algoritmes op klassieke computers met deterministische (1 of 0) bits. De quantumcomputer werd voor het eerst voorgesteld door de natuurkundige Richard Feynman. Hij zag in dat je op basis van quantum-mechanische principes een computer kon bouwen en hij zag simulatie van quantum-mechanische systemen als de belangrijkste toepassing. Dit was een interessante gedachte voor wetenschappers, maar in 1994 liet Peter Shor zien dat je met een quantumcomputer asymmetrische cryptografie kon kraken. Toen werd duidelijk dat een quantumcomputer een grote impact zal hebben op ons dagelijks leven, omdat asymmetrische cryptografie veel gebruikt wordt. Dit soort cryptografie wordt bijvoorbeeld gebruikt voor het beveiligen van internetverkeer via 'https'. Dit algoritme van Shor zorgde voor heel veel belangstelling voor quantumcomputers, maar de bouw van die machines bleek veel moeilijker dan gedacht. Hoewel er inmiddels kleinschalige quantumcomputers bestaan, is er nog geen machine die in staat is Shor's algoritme uit te voeren.

Waarom denken we dan toch dat nu een kantelpunt bereikt is? Naast rekenkracht, kent quantumtechnologie nog twee toepassingen. Die toepassingen zijn al veel verder ontwikkeld en beginnen impact te hebben. We hebben het dan over *quantumcommunicatie* en *quantum sensing*.

Quantumcommunicatie is communicatie gebaseerd op het quantum-mechanische verschijnsel genaamd *verstrengeling*. Twee elementaire deeltjes (zoals elektronen) die verstrengeld zijn met elkaar, hebben toestanden die altijd aan elkaar gecorreleerd zijn. Het aanpassen van het ene deeltje leidt tot onmiddellijke aanpassing van het andere deeltje, ook al zijn die twee deeltjes ver van elkaar verwijderd. Hiermee kan informatie uitgewisseld worden die niet afgeluisterd kan worden. Het maken van verstrengelde deeltjes en ze daarna verplaatsen is technisch zeer ingewikkeld, maar inmiddels zijn meerdere proef-opstellingen gebouwd die dit succesvol doen. Het feit dat deze communicatie niet afgeluisterd kan worden is de belangrijkste drijfveer om hier geld en tijd in te steken. Bedrijven zoals KPN en TNO (en andere referenties) willen een quantuminternet bouwen gebaseerd op deze quantumcommunicatietechnologie. Wereldwijd zijn ook China en de Verenigde Staten koplopers in deze ontwikkeling.

Door gebruik te maken van andere quantum-mechanische principes worden sensoren gebouwd voor navigatie, plaatsbepaling en tijd-meting. Deze verzameling toepassingen wordt quantum sensing genoemd. Deze technologie wordt bijvoorbeeld door het Amerikaanse leger ontwikkeld om wapens en voertuigen autonoom en onafhankelijk van GPS te maken. GSM-netwerken zijn afhankelijk van tijd-synchronisatie tussen de verschillende GSM-masten, en bedrijven die die netwerken bouwen investeren in quantum sensing om hun netwerken robuuster en autonomer te maken.

De grote vooruitgang van quantumcommunicatie en quantum sensing zorgt voor een sterke impuls en het vrijmaken van veel middelen voor quantumtechnologie in het algemeen. En quantum computing, de lastigste van de drie toepassingsgebieden, profiteert hier ook van. Om de voortgang van quantum computing uit te drukken werd soms volstaan met het meten van het aantal qubits dat de computer bevat. We hebben in de afgelopen jaren dit aantal zien groeien van enkelen tot enkele honderden. Om Shor's algoritme te kunnen uitvoeren zijn honderdduizenden qubits nodig dus dat lijkt nog heel ver weg. Het aantal qubits is echter niet een heel goede maat gebleken van vooruitgang. IBM heeft in 2017 het begrip 'quantumvolume' geïntroduceerd. Het quantumvolume is een maat voor de complexiteit van een algoritme dat een bepaalde quantum computer kan uitvoeren. Deze maat hangt niet alleen af van het aantal qubits, maar ook van bijvoorbeeld het aantal operaties dat je op deze qubits kunt uitvoeren voor ze uiteenvallen (qubits zijn erg instabiel, dit is een van de grote problemen van het bouwen van quantumcomputers).

We zien dat wetenschappers en engineers erin geslaagd zijn om het quantumvolume van hun quantumcomputers enorm te laten stijgen[1]. Het punt dat quantumcomputers in staat zullen zijn interessante problemen sneller dan klassieke computers op te lossen lijkt nabij, hoewel niemand weet wanneer dat zal zijn. Dit punt wordt 'quantum advantage' genoemd. Het punt 'quantum supremacy' is al bereikt: dit is het punt waarop een quantumcomputer een zeker algoritme sneller kan uitvoeren dan een klassieke computer. Google claimde dit in 2019 bereikt te hebben[2].

De impact van deze quantum-technologische ontwikkelingen op onze maatschappij, bedrijven en economieën zal groot zijn. Data die banken en andere bedrijven nu versleutelen met cryptografische middelen, zal niet langer vertrouwelijk blijven. Het klassieke internetverkeer zal volledig transparant zijn, ondanks de gebruikte cryptografie. Economieën die beschikken over het veilige quantuminternet en over autonome wapens die zonder GPS hun doelen kunnen vinden zullen een groot voordeel hebben. Maar ook bedrijven die toegang hebben tot een quantumcomputer zullen daarmee een concurrentievoordeel kunnen behalen. Quantumcomputers zijn goed in optimalisatie-problemen. Monte Carlo-simulaties kunnen preciezer uitgevoerd kunnen worden door quantumcomputers omdat geen benaderingen nodig zijn die nu gebruikt worden om ze handelbaar voor klassieke computers te maken. Banken en verzekeraars zullen dit kunnen gebruiken voor prijsoptimalisaties en risicoberekeningen.

Quantumtechnologie zal een grote impact hebben op geopolitieke verhoudingen in de wereld. Het levert kansen op sterkere informatie-beveiliging en betere risicomodellen. Dit levert weerbaardere economieën en samenlevingen op in een tijd van sterke digitalisering. Tegelijkertijd is het een volgende stap in de wapenwedloop tussen geopolitieke blokken. Ook zullen niet alle bedrijven en landen even snel kunnen reageren op de opkomst van deze technologie of er überhaupt de middelen voor hebben. Deze 'digital divide' zal spanningen geven die impact zullen hebben op hun toekomstig succes. In alle mogelijke toekomstscenario's zien we dat quantumtechnologie een factor van betekenis zal zijn. Daarom is het belangrijk dat niet alleen techneuten hiermee aan de slag gaan. Ook beleidsmakers, toezichthouders, bestuurders, actuarissen en iedereen die simulaties, scenario-analyses en risicomodellen ontwikkelt, moeten de toepassingen van deze technologie gaan meenemen in hun toekomstscenario's, modellen en besluitvorming. Quantumtechnologie is een jonge technologie waar nog veel zaken onzeker zijn, maar de impact is verzekerd. ■

1 – https://research.ibm.com/blog/quantum-volume-256

2 – https://www.sciencenews.org/article/google-quantum-supremacy-claim-controversy-top-science-stories-2019-yir

Dr. M. Dekker is Chief Information Security Officer bij ABN AMRO Bank en gasthoogleraar Informatiebeveiliging bij de Universiteit van Amsterdam.