KRACHTPROEF

Kan mensheid de kwantum-computer aan?

Axel Arnbak

Na jaren van speculatie zullen wij over tien jaar terugkijken op 2016 als het jaar dat de kwantumcomputer zich van concept tot realiseerbare uitvinding ontwikkelde. Of het nu tien, twintig of misschien maar drie jaar duurt voordat deze computerexplosie een feit is, de mensheid heeft de consequenties nauwelijks doordacht. Het is goed denkbaar dat de kwantumcomputer huidige hardnekkige geopolitieke en juridische spanningen over gehackte verkiezingen en Snowden-onthullingen niet wegneemt, maar juist versterkt. Als wij niet nu al de economische en sociale gevolgen identificeren en bespreken, zal de verleiding groot zijn de kwantumcomputer eerst en vooral te ontwikkelen voor destructieve militaire doeleinden, in plaats van constructieve civiele toepassingen.

Kwantumcomputers veranderen het fundament van onze huidige informatiesamenleving. Iedere huidige computer — uw pc, ijskast, nieuwe auto en de Zwitserse deeltjesversneller Cern — rekent met bits, cijfers uitgedrukt in nullen of enen. Kwantumcomputers bestaan uit qubits: deeltjes die niet alleen maar één waarde op één moment kunnen aannemen, maar álle denkbare waarden tegelijkertijd — het natuurkundige principe van superpositie. Dit abracadabra begreep ik pas na een verheldering van de Delftse professor Leo Kouwenhoven.

Een normale computer die de uitgang van een doolhof zoekt, probeert één voor één de mogelijke uitwegen totdat de oplossing zich aandient. Een kwantumcomputer kan daarentegen alle oplossingen tegelijkertijd proberen en berekent dus meteen de uitweg. Extreem ingewikkelde wiskundige problemen, zoals weersvoorspellingen of het kraken van versleuteling, zijn nu voor de krachtigste computers onoplosbaar, maar straks voor de kwantumcomputer kinderspel. Kwantumingenieurs likkebaarden bij de gedachte, maar computerbeveiligers en inlichtingendiensten spreken van de naderende 'cryptocalyps'. De encryptie die onze privacy, financiële systemen en staatsgeheimen beveiligt is niet opgewassen tegen de toekomst.

Bovendien verwachten Kouwenhoven en collegae dat wij in de toekomst maar een paar kwantumcomputers nodig hebben om alle computertaken wereldwijd te verrichten. Om de kracht van de sterkste normale computer ter wereld (Titan) te verdubbelen, moet je nu nóg een Titan bouwen — een computer die $ 100 mln kost en even groot is als een voetbalveld. Aan een kwantumcomputer hoef je in theorie maar één chip met een qubit toe te voegen om een exponentiële stijging in computerkracht te realiseren.

Als informatie macht is, dan is de kwantum-computer de droom van iedere machthebber

Tegelijkertijd functioneren kwantumcomputers alleen in sterk gecontroleerde omgevingen waar de temperatuur het absolute nulpunt bereikt (-273,15 graden Celsius). In de toekomst zouden vier of misschien veertig centrale en volledig afgeschermde kwantumcomputers de gehele informatiesamenleving kunnen beheersen. En hebben 'slimme' apparaten — en op termijn allicht de 'slimme' mensen — alleen nog een internetverbinding en een keyboard 2.0 nodig om te interacteren met de omgeving. Een werkende kwantumcomputer zal transparantie van zijn werking en onze privacy, beveiliging en informatieautonomie enorm onder druk zetten.

Nu al lukt het de EU en de VS niet om Trans-Atlantisch datatransport behoorlijk te reguleren en wantrouwen geopolitieke grootmachten elkaars IT-producten. De verleiding van economische en politieke spionage is te groot. Als informatie macht is, dan is de krachtige en gecentraliseerde kwantumcomputer de droom van iedere machthebber. Geen wonder dat Microsoft onlangs een reusachtige joint venture aankondigde met het onderzoekslab Qutech van de gelauwerde kwantumpionier Kouwenhoven in Delft en dat de VS, EU en China ook hevig investeren in de technologie.

Buiten inlichtingendiensten en ingenieurs staan de bredere wetenschap, politiek en het bedrijfsleven nauwelijks stil bij de mogelijkheden van de kwantumcomputer. Natuurlijk zijn er technische uitdagingen en zal het vast niet zo'n vaart lopen. Nu de kwantumcomputer in zicht is, blijken maar een handjevol mensen slim en creatief genoeg om zich überhaupt te kunnen voorstellen hoe je software voor de kwantumcomputer kunt schrijven. De kwantumcomputer zal ook sterkere toepassingen voor privacy en cybersecurity bieden. Maar de dilemma's zitten vooral in hoe de mens en onze sterk uiteenlopende rechtsculturen de kwantumcomputer reguleren. In 2016 stimuleerden grootmachten en ingenieurs de potentie van kwantumcomputers maar zijn brandende ethische kwesties niet eens geformuleerd. Voordat de mens een nieuwe IT-atoombom ontwikkelt, is het in 2017 tijd voor een stevig maatschappelijk debat over de introductie van de kwantumcomputer.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: **@axelarnbak**