# Quantum computing en informatiebeveiliging

Scriptie 9051: Zoëlle Yusufi[redacted]

[redacted]

Scriptiebegeleider: J.C. van Praat

MANAGEMENTSAMENVATTING

Quantum computing zal de cryptografische beheersmaatregelen in bedrijfsprocessen, zeker gaan veranderen. Hoewel quantumcomputers al lang bestaan, is de bestaande quantumtechnologie nog niet krachtig genoeg om de huidige cryptografische algoritmes te doorbreken. Vooraanstaande experts schatten dat de kans 50% of meer is dat RSA-2048 binnen 15 jaar, in 24 uur, door een quantum computer wordt gebroken. Dat wil zeggen dat een quantum computer een getal van 2048 bits kan ontbinden in 24 uur (Mosca & Piani, 2020).

Quantum computers zullen de meest populaire cryptografische systemen met public keys breken, waaronder RSA, DSA en ECDSA. Hiermee staan we aan de vooravond van een technologische revolutie. Deze revolutie kan een bijdrage leveren aan de oplossing van maatschappelijke vraagstukken, zoals inzichten die nu verborgen liggen in de enorme hoeveelheden ongestructureerde data die we als samenleving produceren. Tegelijk brengt het ook nieuwe risico's met zich mee op het gebied van privacy, veiligheid, economische ongelijkheid en geopolitieke verhoudingen.

*Bevindingen*

Organisaties zijn nog bezig met de begripsvorming van quantum-computing en zitten in een aanloopfase. Uit het praktijkonderzoek komt naar voren dat organisaties nog niet echt bezig zijn met het treffen van voorbereidingen naar quantum-veilige informatiebeveiligingssystemen.

*Conclusie*

Om de juiste beslissingen te kunnen nemen voor (optimalisatie van) de bedrijfsvoering, ontwikkeling, beheer, regelgeving en investeringen in quantum-veilige informatiebeveiligingssystemen moet het management worden geïnformeerd over de impact van quantum computers en de oplossingen voor cryptografie. Organisaties dienen een ketenbrede risicoanalyse uit te voeren en te inventariseren waar in de waardeketen welke cryptografische oplossingen worden gebruikt om daarna een actieplan te maken voor quantum-veilige oplossingen. In deze scriptie worden concrete voorstellen gedaan voor de beheersing van de quantum-risico's.

Een belangrijke overweging voor organisaties voor het wanneer te starten zijn kosten. Organisaties kunnen de kosten van de overgang naar een quantum-veilige cryptografie verminderen door al in een vroeg stadium aan leveranciers interesse te tonen in quantum-veilige producten en crypto-agility (flexibiliteit in cryptografische algoritmen en sleutellengten) te vereisen voor alle producten die vanaf nu moeten worden gekocht (Muller & Van Heesch, 2020).

# Inhoudsopgave



## Lijst van Tabellen en Figuren

# 1 Inleiding

Quantumtechnologie, cryptografie en de auditprofessie omvatten een eigen werkveld en vereisen vaak een andere achtergrond en vaardigheden. Echter, met het gebruik van quantum computing wordt de aantrekkingskracht tussen de drie voelbaar.

Quantumcomputers hebben het potentieel om berekeningen sneller uit te voeren dan conventionele (super)computers. Een quantumcomputer kan bijvoorbeeld zorgen voor een ongekende ontwikkeling op het gebied van Artificial Intelligence en is in staat om met een enorme snelheid parallelle berekeningen uit te voeren op een dataset die met een conventionele (super)computer niet te verwerken is (Kurzgesagt 2019). Daarmee zal quantum computing ook van invloed zijn op cryptografie (versleuteling) zoals die hedendaags wordt gebruikt, waardoor de noodzaak voor post-quantumcryptografie.

Experts vermoeden nu meer dan ooit dat quantum computing Artificial Intelligence op een bepaald niveau zal gaan veranderen. Zo wijzen analisten bijvoorbeeld op de natuurlijke synergie tussen quantum computing en Artificial Intelligence als reden waarom quantum machine learning uiteindelijk de beste klassieke vorm van machine learning zal zijn (Swayne, 2020). Onderzoek naar onder meer quantum-algoritmes en Artificial Intelligence beschrijft dat quantumcomputers een snelle analyse en integratie van enorme datasets mogelijk zullen maken. Dit zal de mogelijkheden voor machine learning en Artificial Intelligence niet alleen verbeteren maar ook transformeren (Ying, 2010).

Quantumcomputers zullen de meest populaire cryptografische systemen met public keys breken, waaronder RSA, DSA en ECDSA. Als gevolg hiervan zal voor alle algoritmes met een secret key gebruik moeten worden gemaakt van ten minste een 256-bits sleutel en alle huidige algoritmes voor public keys zullen moeten worden vervangen door algoritmes die bestand zijn tegen de aanvallen die mogelijk worden gemaakt door de quantumcomputer (Muller & Van Heesch, 2020). Hiermee staan we aan de vooravond van een technologische revolutie. Deze revolutie kan een bijdrage leveren aan de oplossing van maatschappelijke vraagstukken, maar brengt tegelijk nieuwe risico's met zich mee.

De ontwikkeling van quantumtechnologie heeft niet alleen een technologische en economische impact, maar het heeft ook ethische en juridische aspecten. In deze scriptie wordt de nadruk gelegd op de ethische en juridische kant vanuit het perspectief van dataprotectie, wet- en regelgeving en standaarden. Daarnaast wordt de huidige auditprofessie in het kader van deze nieuwe ontwikkelingen besproken. Naast een analyse van het onderwerp wordt in het kort stilgestaan bij de geschiedenis van het onderwerp, een bespreking van quantum computingbegrippen zoals verstrengeling en het gebruik daarvan in algoritmes, en vermoedens ten aanzien van de vooruitzichten en valkuilen.

In deze scriptie worden de relevante theoretische concepten en modellen, die in de literatuur worden gepresenteerd, vergeleken met de in de praktijk gangbare situaties. Daarnaast wordt onderbouwd aangegeven of in de onderzochte praktijksituatie de in de literatuur beschreven theoretische concepten en modellen tekortschieten.

Het vervolg van de scriptie bestaat uit vier secties. Eerst wordt de literatuur besproken, waarna wordt ingegaan op de gebruikte methode. Vervolgens wordt de praktijksituatie gepresenteerd en gebaseerd op de besproken literatuur. Ten slotte worden de resultaten besproken, gevolgd door een conclusie.

# 2 Probleemstelling

Quantum computing kent verschillende uitdagingen. Een uitdaging met veruit de meeste impact op niet alleen het bedrijfsleven maar ook de maatschappij is de bedreiging voor cryptografie.

## *§2.1 Terreinafbakening*

In de literatuur worden diverse invalshoeken besproken om quantum computing te implementeren. Deze scriptie is vooral toegespitst op de impact van quantum computing op cryptografie in de informatiebeveiligingsprocessen en bedrijfsapplicaties in organisaties. Dit leidt tot de volgende primaire hoofdvraag:

*Hoe houden organisaties kansen en bedreigingen van quantum computing op informatiebeveiliging beheersbaar?*

Om hierop antwoord te kunnen geven, zijn vier deelvragen geformuleerd die volgens de Case study research, (Yin, 2009) iteratief worden onderzocht.

## *§2.2 Deelvragen*

Om antwoord te kunnen geven op de primaire hoofdvraag zijn in de 'plan' fase (Yin, 2009), op basis van de geschreven literatuur, vier deelvragen geformuleerd. De eerste twee deelvragen gaan in op de implementatie van quantum computing in het licht van cryptografie, data en Artificial Intelligence. De derde deelvraag gaat in op de praktijksituatie. Tot slot wordt de invloed van quantum computing in het licht van de huidige standaarden en auditprofessie onderzocht:

1. *Wat zijn de kansen en bedreigingen van quantum computing in de context van cryptografie?*

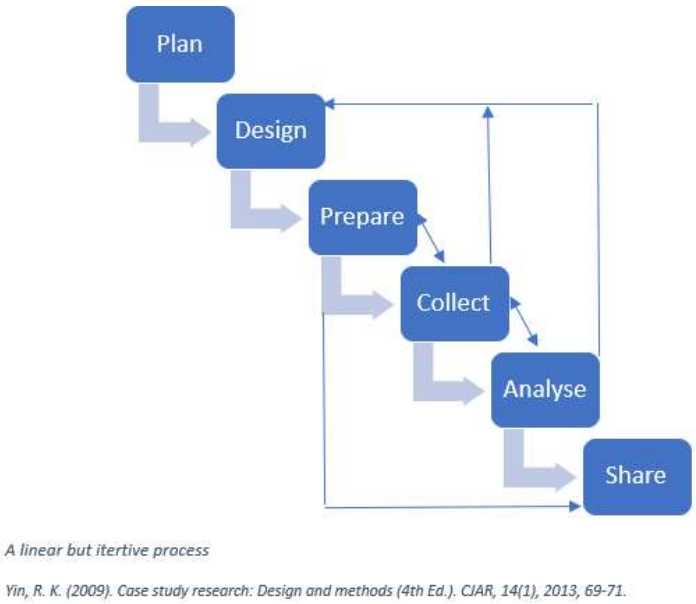
2. *Hoe verschilt de implementatie van post-quantum cryptografie op conventionele computers ten opzichte van andere, veel toegepaste cryptografische methoden?*

3. *Hoe beïnvloedt quantum computing de informatiebeveiliging in bedrijfsprocessen?*

4. *Zijn er algemeen aanvaardbare standaarden voor de toepassing van quantum computing en wat is de rol van de auditprofessie?*

## *§2.3 Onderzoeksmethode*

De onderzoeksmethode en opbouw van het onderzoek volgt de iteratieve aanpak van Robert K. Yin, beschreven in Figuur 1 'Case study research, design and methods', 4th edition (Yin, 2009).




Figuur 1: Case study research (Yin, 2009)

*2.3.1* 'Plan' (Hoofdstuk 2) bevat de bepaling van de onderzoeksvragen binnen het beschreven kader, de scope en de literatuurstudie. Voor deze scriptie wordt, naast literatuuronderzoek, ook gebruik gemaakt van interviews.

*2.3.2* 'Design' (Hoofdstuk 3) levert de literatuurstudie op en de blauwprint van een interview teneinde stellingen bij organisaties en experts te verifiëren. Naast aandacht voor de kwaliteit en de betrouwbaarheid van de procedures en uitkomsten, is de vorm van de vraagstelling relevant. Om een juiste verdeling te krijgen tussen de bijdrage van experts en indien denkbaar de antwoorden in het licht van een overkoepelende groepsopinie te stellen.

*2.3.3* 'Prepare' (Hoofdstuk 4) beslaat de opzet van het interview. Daarnaast wordt

een pilot uitgevoerd om de werking en de inhoudelijke effectiviteit van de gekozen methodes te evalueren. Voor publicatie van de uitkomsten wordt toestemming gevraagd. Indien nodig vinden correcties plaats in de opzet of in de vraagstelling.

*2.3.4* 'Collect' (Hoofdstuk 4) beslaat de periode van de uitvoering van de interviews. Dit zijn tussentijdse (inhoudelijke) response-metingen en het versturen van herinneringen om eventueel bij te sturen. Bovendien wordt een database aangelegd ten behoeve van alle evidence, gecollecteerde data en ter onderbouwing van de betrouwbaarheid van de gevormde conclusies. Alle interviews worden opgenomen. De interviews worden getranscribeerd en woordelijk uitgewerkt met behulp van de audio opnamen die de adviezen en meningen van experts omvatten.

*2.3.5* 'Analyze' (Hoofdstuk 4) omvat een detailanalyse van de afgenomen interviews en van de verkregen input op elk van de (deel)vragen en ingenomen stellingen. Afhankelijk van de input van de experts worden de deelvragen en stellingen en voorlopige aanbevelingen eventueel aangepast. Dit is relevant voor de inhoud van de uiteindelijke conclusie. Als kwaliteitscontrole worden met experts aanvullende interviews gehouden naar aanleiding van de voorlopige uitkomsten van het 'Analyze'-proces. Het aantal interviews is mede afhankelijk van de analyse-uitkomsten. Hierbij wordt in acht genomen of experts de voorgedragen vraagstellingen verwerpen of steunen. Bij de terugkoppeling met betrekking tot de 'Collect'-fase ontvangen experts inzicht in de uitkomsten van de voorlopige stellingen en analyses. Dit is relevant voor de inhoud van het uiteindelijke oplossingsvoorstel. Hierbij worden de uitkomsten ook kwantitatief belicht.

Voor de uitwerking en analyse van de interviews wordt in drie fases gecodeerd: open (labelen), axiaal (clusteren) en selectief (hiërarchie aanbrengen binnen de codering, het verklaren van verschillen, overeenkomsten en conclusie) volgens de methode beschreven door Gioia et al. (2012).

*2.3.6* 'Share' omvat de vastlegging van de afstemming met betrekking tot de interviews met elke expert, de gerapporteerde resultaten van de geïnterviewden en geënquêteerden, de verspreiding van de scriptie aan

belangstellenden en activiteiten gericht op aanmoediging van wetenschappelijk onderzoek naar het thema van deze scriptie.

Om de vier deelvragen te kunnen beantwoorden wordt een literatuuronderzoek uitgevoerd. Daarna wordt op basis van een praktijkonderzoek, 'analyze' (Yin, 2009), onderzocht of de literatuurstudie op basis van het uitgevoerde praktijkonderzoek wordt onderkend.

# 3 Literatuuronderzoek

Het literatuuronderzoek is onderdeel van de ‘design’ fase van (Yin, 2009) en richt zich op de kansen en bedreigingen die quantum computing met zich meebrengt voor de beheersing van informatiebeveiliging, in het bijzonder cryptografie, in bedrijfsprocessen. Eerst wordt ingegaan op de begripsvorming, de historie en de verschillende toepassingen van quantum computing. Vervolgens wordt gekeken naar de invloed die quantum computing zal hebben op onder meer informatiebeveiliging, data, cryptografie, standaarden en controle zoals die hedendaags wordt toegepast.

## *§3.1 Begripsvorming en de historie*

De technologie en de ideeën over de toepassing van quantumtechnologie bestaan al enige tijd, maar ten gevolge van een aantal doorbraken wordt nu aan concrete toepassingen gewerkt. Om het mechanisme achter quantum computing uit te kunnen leggen, wordt eerst stilgestaan bij de term ‘quantummechanica’. Dit kan het beste worden uitgelegd als een set vergelijkingen die gehanteerd worden om de werkelijkheid te beschrijven (Kraaijvanger, 2018). Het woord ‘quantum’ komt van quantummechanica, de wetenschappelijk studie naar het gedrag van atomaire en subatomaire deeltjes. Quantummechanica ontstond in het begin van de negentiende eeuw als een reactie op wetenschappelijke theorieën die niet konden worden verklaard. Voorlopers hiervan waren prominente fysici zoals Max Planck, Albert Einstein, Geïnterviewde: Bohr en Erwin Schrödinger.

Alhoewel vooraanstaande fysici dit gedrag in detail beschreven, wordt de essentie van quantummechanica al genoemd in de Koran, die in de zevende eeuw al herhaaldelijk spreekt over alam-al-ghaib (de verborgen dimensie van de werkelijkheid). De quantumbeschrijving van de werkelijkheid maakt een einde aan het tijdperk van het materialisme, in die zin dat het een bestaan vereist van een niet-fysieke geest achter het fysieke brein. Nu ruim weer een eeuw later staat quantumtechnologie aan de vooravond van een nieuwe quantumrevolutie.

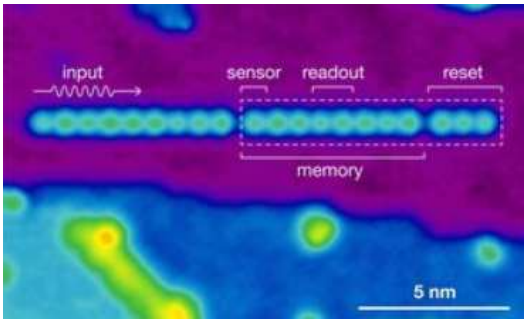
In quantummechanica wordt alles beschreven in golven; geen fysieke golf, maar meer een gestandaardiseerde wiskundige vergelijking. Quantumtechnologie is gebaseerd op

deze natuurwetten die het gedrag van een 'quantum', de kleinste, ondeelbare hoeveelheid van een grootheid die bij een interactie betrokken kan zijn, beschrijven (Klitzing, 2004). Zo kunnen quantumdeeltjes op microniveau verschillende waarden (twee) tegelijkertijd hebben en zich onder bepaalde voorwaarden gedragen als één, ongeacht hun onderlinge afstand. Deze eigenschappen van de kleinste deeltjes vormen de basis voor quantum computing, quantumsimulatie (rekenen), quantum sensing (meten) en quantum internet (communiceren) (ECP, 2019). Dit biedt veel mogelijkheden in het licht van quantum computing en het oplossen van rekenproblemen, ook wel Quantum Supremacy genoemd. Boixo et al. omschrijven 'Quantum Supremacy' als het oplossen van een goed gedefinieerd rekenprobleem op een quantumprocessor in een korte tijd, bijvoorbeeld een seconde, hetgeen door een conventionele computer niet binnen redelijke tijd, bijvoorbeeld tien jaar, kan worden opgelost (Boixo et. al, 2018). Dit paradigma is bedoeld om deze methode direct te gebruiken om berekeningen uit te voeren of de rekenefficiëntie te vergroten. Sommige problemen kunnen theoretisch op een quantumcomputer exponentieel sneller worden opgelost dan op een klassieke computer (Kasivajhula, 2006).

## *§3.2 Verschillende toepassingen van quantumtechnologie*

Quantumtechnologie heeft verschillende toepassingen, bijvoorbeeld in microscopisch kleine sensoren (quantum nano science) en computers met een enorme rekenkracht (quantumcomputers), radiofrequency-technologie (communicatietechniek die werkt op basis van radiogolven), bigdata-analyse, veilige quantumnetwerken, IOT, informatiebeveiliging en cryptografie. Deze technologieën zullen leiden tot doorbraken op onder andere het gebied van digitalisering, medicijnen, materialen en cybersecurity. De TU Delft heeft in mei 2020 een sensor ontwikkeld van slechts elf atomen groot. Ter vergelijking, in een nanometer passen ongeveer vijf atomen. En 1000 nanometer = 0,00010 centimeter. Figuur 2 [1] is een voorbeeld van quantum nano science toegepast in een microscopisch kleine sensor. De sensor kan magnetische golven opvangen en heeft een antenne, een uitleesmogelijkheid, een geheugeneenheid en een resetknop.

[1]Herdrukt van "Researchers build sensor consisting of only 11 atoms", door Communication TNW, 2020, 25 mei. Geraadpleegd van https://www.tudelft.nl/en/2020/tnw/researchers-build-sensor-consisting-of-only-11-atoms




*Figuur 2: Grafische weergave sensor* [1]

Het onderzoek van TU Delft is gericht op het gedrag van magnetische golven, met als doel het gebruik van deze magnetische golven in groene ICT-toepassingen (Wallucks et al., 2020). Met groene technologie kan niet alleen geld worden bespaard, maar kan ook de CO2-voetafdruk worden verlaagd.

De theorie die aan deze sensor ten grondslag ligt, beschrijft dus gedrag van de kleinste quantumdeeltjes, waarbij deeltjes zich soms gedragen als golven en golven zich soms gedragen als deeltjes, hetgeen alleen op atomair en subatomair niveau merkbaar is. Wetenschappelijk onderzoek onderschrijft ook dat deeltjes zich kunnen gedragen alsof ze op twee plekken tegelijkertijd zijn, ook wel superpositie genoemd (Boixo et. al, 2018). Dit betekent dat de deeltjes die zich op afstand van elkaar bevinden met elkaar kunnen communiceren zonder meetbare signalen door de lucht te sturen. Verandering van een deeltje betekent een verandering in het verstrengelde deeltje. Dit wordt ook wel verstrengeling genoemd. Verstrengeling is vooral interessant vanuit het aspect van dataverbindingen.

Wetenschappers van de TU Delft lieten in 2015 zien dat er sprake is van ‘verstrengeling van deeltjes’, een telepathische invloed tussen quantumdeeltjes (Merali, 2015). Met andere woorden, de waarneming van het ene deeltje heeft gevolgen voor het andere deeltje. Dit betekent dat dit ook geldt als dat andere deeltje zich op een grote afstand van het ene deeltje bevindt. Het is ze gelukt om deeltjes op 1,3 km afstand te laten verstrengelen. In theorie zou dit betekenen dat de onderlinge afstand lichtjaren groot kan zijn en de deeltjes toch verstrengeld zijn.
Dat weerlegt de universele regel dat niets sneller kan reizen dan de snelheid van licht.

Terug naar een computer. Een computer werkt met kleine elektronische schakelaars; dit zijn transistors die slechts twee standen kennen, een 0 of een 1. Des te kleiner een transistor, hoe meer ervan gebruikt kunnen worden in een computer en des te sneller een computer werkt. Daarmee staan conventionele computers aan de grenzen van de gegevensverwerkingskracht en data blijft groeien. De wet van Moore stelt dat het aantal transistors, en daarmee de rekenkracht, op geïntegreerde schakelingen elke twee jaar verdubbelt (Schaller, 1997). Door de omvang van transistors met bestaande nanotechnologie te verkleinen, kunnen ingenieurs meer op een microprocessor plaatsen, waardoor de rekenkracht van de processor wordt vergroot. Dit proces kan niet eeuwig doorgaan. Geschat wordt dat ingenieurs ergens in de komende twee decennia, in het huidige tempo, met het probleem worden geconfronteerd om iets te bouwen dat kleiner is dan een atoom. Dit is zover als ons huidige computerparadigma ons zal brengen.

Het verschil tussen conventionele computers en quantumcomputers is dat conventionele computers informatie in de vorm van bits opslaan. Deze bits kunnen zoals hierboven toegelicht slechts één getal tegelijk weergeven.
In een quantumcomputer zijn de bits vervangen door ‘quantumbits’ (Qbits).

In Figuur 3 is een 50-qubit quantumcomputer van IBM opgenomen. Van boven naar beneden koelt het systeem geleidelijk af.
De draden voeren ondertussen RF-frequentiesignalen naar de chip. Deze worden vervolgens in kaart gebracht op de qbits en voeren het gewenste programma uit. De bedrading is zo ontworpen dat er geen externe ruis, inclusief warmte, wordt getransporteerd naar de quantumcomputerchip aan de onderkant.

*Figuur 3: 50-qubit quantumcomputer IBM* [2]

Quantumdeeltjes gedragen zich op de nanoschaal totaal anders. Dit houdt in dat een deeltje op meerdere plaatsen tegelijk kan zijn. Bij een quantum computer is de informatie over de plek van een deeltje niet meer binair. Een deeltje bevindt zich dan niet meer op één plek en kan zowel op plek X als op plek Y zijn. Daarmee kan

[2] Herdrukt van “This is what a 50-qubit quantum computer looks like”, door Summers, N., 2018, 10 januari. Geraadpleegd van https://www.engadget.com/2018-01-09-this-is-what-a-50-qubit-quantum-computer-looks-like.html?

worden gesteld dat het deeltje een superpositie heeft aangenomen, waarin elk getal met een bepaalde kans voorkomt (Bloemink, 2018b).

In de volgende tabel staan een aantal van de belangrijkste verschillen tussen conventionele computing en quantum computing samengevat (Eizerman et al.,2005; Steane, 1998; Hey, 1999; Knill, 2010; Seife, 2005).

*Tabel 1: Conventionele computing en quantum computing*

| ***Conventionele computing*** | ***Quantum computing*** |
|---|---|
| Conventioneel computergebruik is gebaseerd op natuurkunde. Het is gebaseerd op het feit dat elektrische circuits zich op een bepaald moment in een enkele toestand bevinden, aan of uit. Voorbeelden van conventionele computers zijn: mainframe computers, mobiele telefoons, PC's, MAC, etc. | Quantum computing is gebaseerd op de quantummechanica, zoals superpositie en verstrengeling, het fenomeen waarbij het mogelijk is om in meer dan één toestand tegelijk te zijn. Een voorbeeld van quantum computing is een quantumcomputer. |
| Conventionele computing gebruikt transistors en is gebaseerd op 'bit' dat gebaseerd is op spanning of lading, deze is binair, uit is 0 en aan is 1. Een bit kan alleen één van deze staten hebben, niets ertussenin. Een bit wordt gemanipuleerd via de klassieke computingregels, 'gates', zoals not, and, or, etc. Een PC is gemaakt van biljoenen 'logic gates' en een logic gate is gemaakt met vele transistors. | Quantum computing gebruikt quantumtransistors. Informatieopslag is gebaseerd op quantum bit of 'qubit', dat is gebaseerd op de spin van elektronen of polarisatie van een enkel foton. Quantum computing gebruikt qbits, dat wil zeggen 0, 1 en een superpositietoestand van zowel 0 als 1 om informatie weer te geven. |
| Op conventionele computers wordt de gegevensverwerking uitgevoerd in de Central Processing Unit of CPU, die bestaat uit een Arithmetic and Logic Unit (ALU), processorregisters en een besturingseenheid. | In quantum computers wordt de gegevensverwerking uitgevoerd in de Quantum Processing Unit of QPU, die bestaat uit een aantal onderling verbonden qbits. |
| Klassieke computing kan worden uitgedrukt in N bits. | Quantum computing kan worden uitgedrukt in $N = 2^n$ bits. |

Quantum computers zijn ontworpen om enorme hoeveelheden data te beheren.
Met elke iteratie van het ontwerp van een quantum computer en verbeteringen aan de code voor de correctie van quantumfouten, kunnen programmeurs het potentieel van Qbits om exponentieel meer gegevens te beheren, beter beheersen. Anders gezegd, het toevoegen van één qubit maakt een computer twee keer zo snel (Swayne, 2020). Qbits kunnen worden gezien als een quantum-mechanische versie van een klassieke databit. Shannon (1948) definieert een bit als volgt: "de kleinste eenheid van informatie, namelijk een symbool of signaal dat twee waarden kan aannemen: aan of uit, ja of nee, hoog of laag, geladen of niet-geladen. Het binaire talstelsel stelt deze

waarden voor met 1 en 0". In de volgende tabel is een voorbeeld van het potentieel van Qbits opgenomen, het voorbeeldeffect van het toevoegen van één Qbit.

*Tabel 2: Het potentieel van Qbits*

| ***2 Qbits*** | | ***3 Qbits*** | |
|---|---|---|---|
| 00<br>01<br>10<br>11 | 4 simultane waarden | 000<br>001<br>010<br>011<br>101<br>100<br>110<br>111 | 8 simultane waarden |

Dit biedt mogelijkheden voor Artificial Intelligence. Quantum machine learning is hierdoor bijvoorbeeld efficiënter dan klassieke machine learning voor bepaalde modellen die intrinsiek moeilijk te leren zijn met conventionele computers (Swayne, 2020). Deze mogelijkheden maken quantum computers interessant voor een breder publiek, waaronder inlichtingendiensten, cryptografen en veiligheidsdiensten. Quantum computers bestaan al, alleen is de bestaande technologie op dit moment nog niet krachtig genoeg om cryptografie te doorbreken (TNO, 2020)

*Quantum computing en digitale data(innovaties)*

De impact van digitale innovaties, big data en Artificial Intelligence op organisaties heeft niet alleen een bedrijfseconomische impact maar ook een maatschappelijke en sociale impact. Uitwisseling van informatie is in sterke mate versneld door nieuwe technologieën. Waar bijvoorbeeld vroeger het fotorolletje werd gebruikt, worden foto's tegenwoordig via het internet gedeeld door gebruik te maken van een mobiele telefoon en uploads naar de cloud. Een ander voorbeeld zijn digital twins. De granulariteit van data en IOT maken het mogelijk om wanneer je wilt, overal toegang te krijgen tot informatie. Digitalisering vervangt vele fysieke spullen zoals een portemonnee (door bijvoorbeeld Apple Pay) en andere goederen en diensten. Technologie wordt laagdrempelig en in grote volumes, wereldwijd beschikbaar waardoor iedereen er gebruik van kan maken.

Mensen zijn gewend lineair te denken, waardoor exponentiële technologische veranderingen een bestaand businessmodel onverwacht verstoord. In werkelijkheid stijgt een ontwikkeling exponentieel waardoor de wereld zoals wij die kennen

'bedrieglijk' is. Geld als monetaire eenheid verdwijnt; men betaalt met data. Digitale innovaties creëren nieuwe markten en ontwrichten bestaande markten en verdienmodellen. De wereld wordt in toenemende mate bedrieglijk en daardoor ontwrichtend. Big data en Artificial Intelligence tools met behulp van quantum computing zullen datgene in data ontdekken waarvan we nog niet weten dat we het niet weten.

*Quantum computing en Artificial Intelligence*

Artificial Intelligence verwijst naar het doel van machines die denken zoals mensen en daarom ook kunnen werken als mensen. Het is in de basis interdisciplinair en een bloeiend veld in datawetenschap geworden, Artificial Intelligence integreert ideeën uit de filosofie, wiskunde, statistiek, taalkunde, psychologie en neurowetenschappen. Quantumkunstmatige intelligentie (QAI) is een interdisciplinair veld dat zich richt op het bouwen van quantumalgoritmes voor het verbeteren van computertaken binnen kunstmatige intelligentie, inclusief subvelden zoals machine learning (Tavernier, 2001). Dit dankzij een enorm en intrinsiek parallellisme dat mogelijk wordt gemaakt door superpositionering en verstrengeling van verschillende stukjes informatie (Acampora, 2019).

Artificial Intelligence wordt vaak gebruikt als overkoepelende term voor vooruitgang in specifieke technologieën en benaderingen zoals machine learning en natural language processing. In dit scenario heeft de recente implementatie van quantumalgoritmes voor machine learning geleid tot een golf van steeds geavanceerdere resultaten die laten zien hoe quantumcomputers efficiënter kunnen zijn in het oplossen van problemen op het gebied van kunstmatige intelligentie, sneller dan hun klassieke tegenhangers (Biamonte et al., 2017; Schuld et al., 2015; Dunjko & Briegel 2018; Schuld & Petruccione, 2018). Het voordeel van quantum computing toegepast op machine learning is te wijten aan de exponentiële toename van het aantal dimensies dat quantum machine learning kan verwerken in vergelijking met klassieke machinelearning-algoritmes (Havlíček et al., 2019 ). Het kenmerkende van Artificial Intelligence is dat bij Artificial Intelligence het niet de mens is die de bepaalde rekenregels bepaald. Naar Artificial Intelligence wordt verwezen als technologie die taken kan uitvoeren die vaak worden geassocieerd met intelligentie op het niveau van

(of slimmer dan) intelligente wezens en daarom bij bepaalde taken soms beter kan werken dan mensen.

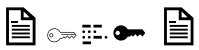
Een aantal uitdagingen die komen kijken bij een toepassing hiervan zijn onder meer de Europese privacywetten inzake datagebruik en gegevensverwerking. Om met behulp van Artificial Intelligence een waardevolle bijdrage te kunnen leveren aan de maatschappij c.q. economie zijn juridische en ethische kaders nodig (TNO, 2020). Organisaties kunnen zich afvragen welke wetgeving er geldt voor quantum computing en hoe dit dan zit met de rechten en verplichtingen met betrekking tot bijvoorbeeld privacy, veiligheid en intellectueel eigendom (TNO, 2020). Om van Artificial Intelligence te kunnen profiteren, zijn een zorgvuldige afweging, ethische normen en voorschriften nodig. Een quantum computer zal daaraan weinig veranderen (Jong et al., 2019).

## *§3.3* Quantum computing en cryptografie

Om te begrijpen hoe cryptografie beïnvloed wordt door quantum computing worden eerst de belangrijkste en veelgebruikte cryptografische oplossingen, in de vorm van sleutelalgoritmes, toegelicht. Deze sleutelalgoritmes zijn systemen voor een digitale beveiliging voor de uitwisseling van data. Dit worden ook wel asymmetrische sleutelalgoritmes genoemd en zijn *in tabel 5 van bijlage 1* toegelicht. Hoewel door de jaren heen veel algoritmes zijn ontwikkeld, zijn de meest gebruikte en algemeen aanvaarde asymmetrische sleutelalgoritmes RSA, DSA en ECC. Die kunnen worden gecombineerd met RSA voor veiligere bescherming (Parms, 2021).

Cryptografie is een methode om moderne wiskundige regels te gebruiken bij het opslaan en verzenden van data in een bepaalde vorm, zodat alleen de ontvangers deze kunnen verwerken en lezen. Encryptie (versleuteling) hoort bij cryptografie; het is een procedure waarbij een bericht wordt gecodeerd in een extensie die onleesbaar is voor een onderschepper. Een platte tekst kan worden gecodeerd naar een cijfertekst en daarna via een communicatiekanaal worden verstuurd. Een onderschepper kan de platte tekst niet verstoren. Wanneer de tekst de ontvanger heeft bereikt, wordt de cijfertekst ontsleuteld tot de oorspronkelijke platte tekst (Parms, 2021).

Cryptografie speelt een grote rol in versleuteling van data, het afschermen van informatie en het daarmee waarborgen van vertrouwelijkheid. Cryptografie zorgt ervoor dat partijen met elkaar op een veilige manier kunnen communiceren en dat de authenticatie van informatie gewaarborgd is. Dit geldt voor alle digitale communicatie, om verbindingen op een veilige manier tot stand te laten komen, worden verschillende encryptiemethoden gebruikt. Dit is zodat een onderschepper van de informatie het bericht niet kan ontcijferen en lezen, omdat het bericht versleuteld (encrypted) is. Encryptie wordt toegepast in de informatiebeveiliging van het dataverkeer en wordt onderverdeeld in twee groepen:

- symmetrische encryptie dat één dezelfde sleutel gebruikt: 
- asymmetrische encryptie gebruikt twee verschillende sleutels, één publieke en één private sleutel: 

Ten grondslag aan encryptie zitten wiskundige algoritmes die voor de huidige conventionele computers onoplosbaar zijn. In het onderstaand tabel zijn cryptografische algoritmes opgenomen die door organisaties veel gebruikt worden.

In de praktijk worden twee populaire versleutelingsschema's gebruikt om de communicatiebeveiliging in symmetrische en asymmetrische versleuteling aan te scherpen (Shor, 1994; Grover, 1996). Een belangrijk concept hierbij zijn algoritmes. Een versleutelingsalgoritme is een reeks wiskundige regels voor de uitvoer van versleuteling van gegevens. Door het gebruik van een algoritme wordt er data gemaakt in de versleutelde tekst en is een sleutel vereist om de data in originele vorm om te zetten. Dit gaat terug naar het principe van cryptografie dat al tijden wordt gebruikt bij informatiebeveiliging in communicatiesystemen (Parms, 2021).

Gekozen kan worden voor symmetrische en asymmetrische versleuteling. Waarvan asymmetrische versleuteling (nieuwer) het meest wordt gebruikt in vooral dagelijkse communicatiekanalen, met name via internet. Populaire asymmetrische encryptiemethoden zijn bijvoorbeeld RSA, DSA ECC en 'Elliptic Curve'-technieken. Om een cryptografisch systeem met public keys te laten werken, is een set algoritmes nodig. De standaard die in gebruik is sinds de jaren zeventig is afhankelijk van de vermenigvuldiging van twee grote priemgetallen.

Een efficiënt algoritme om het probleem van de factorisatie van grote gehele getallen op te lossen, maakt het RSA-cryptosysteem onveilig en, om deze reden, vormen quantumcomputers een zeer ernstige bedreiging voor dit soort veelgebruikte cryptosystemen (TNO, 2020).

Asymmetrische sleutelalgoritmes blijken in de praktijk vaak als coderingsschema de voorkeur te hebben. Met de komst van mobiele apparaten die worden gebruikt voor privétransacties, worden veiligere coderingsschema's zeer wenselijk. ECC-cryptografie helpt om een beveiligingsniveau tot stand te brengen dat gelijk is aan of groter is dan RSA of DSA, de twee meest algemeen aanvaarde versleutelingsmethoden – en het doet dit met minder computationele overhead en vereist minder verwerkingskracht (Parms, 2021).

Om het versleutelde bericht te ontcijferen, zijn de twee afzonderlijke getallen nodig. Alleen de ontvanger kan de berichten ontcijferen, omdat die als enige de private key kent (twee afzonderlijke factoren). Zolang een eventuele onderschepper deze grote getallen niet kan "ontbinden", werkt deze methode goed. De berekeningen die nodig zijn om encryptie (versleuteling) te verbreken, zijn behoorlijk complex waardoor zelfs de snelste computers ter wereld hier jarenlang over doen. Door middel van snellere processoren zijn veel versleutelingsmethoden al gekraakt en daarmee onveilig geworden. Door quantum computing en quantumcomputers raakt het onveilig worden van veilige encryptiemethoden in een stroomversnelling. Een quantum computer zal namelijk deze asymmetrische encryptiemethoden doorbreken (ECP, 2019). Vooraanstaande experts schatten dat de kans 50% of meer is dat RSA-2048 binnen 15 jaar, in 24 uur, door een quantum computer wordt gebroken (Mosca & Piani, 2020).

Met de middelen om versleutelde communicatie nu te archiveren, kan deze communicatie in de nabije toekomst retrospectief worden ontcijferd met quantum computing; "store now decrypt later" (Swayne, 2020).
Er zijn twee quantum-algoritmes die het beveiligingsniveau van de bestaande manier van encryptie kunnen doorbreken, het algoritme van Shor en het algoritme van Grover. Het algoritme van Shor doorbreekt asymmetrische encryptie zoals RSA, ECC en Diffie Hellman door het oplossen van het discrete log probleem. Het algoritme van Grover maakt symmetrische encryptie, zoals AES zwakker (Roetteler et al., 2017).

De belangrijkste toepassingen van cryptografie met public keys zijn voor digitale handtekeningen en het vaststellen van sleutels (Chen et al.,2016).
De Algemene Inlichtingen- en Veiligheidsdienst en het Nationaal Cyber Security Centrum (AIVD, 13 april 2015) wijzen in publicaties erop dat organisaties en bedrijven in Nederland zelf verantwoordelijk zijn voor hun digitale beveiliging (ECP, 2019). Dit betekent dat organisaties moeten begrijpen wat de impact is van de quantumdreiging op hun bedrijfsactiviteiten. Daarom is het relevant dat 'quantum-veilige' cryptosystemen worden ontworpen om digitale handelingen op een veilige manier uit te kunnen blijven voeren (ECP, 2019).
Het meest bekende quantumcryptografische protocol is Quantum Key Distributie (QKD), waarmee twee gebruikers gezamenlijk via een quantumlink (een point-to-point quantumnetwerk) een sleutel genereren, welke vervolgens gebruikt wordt om gegevens te versleutelen. Bij QKD wordt het direct opgemerkt wanneer iemand anders de quantum-informatie heeft bekeken (Vermaas et al., 2019).

De opkomst van post-quantumcryptografie bij de beveiligingsinstanties, zoals de National Security Agency (NSA) is een voorbeeld, daarnaast beginnen ook bedrijven oplossingen te eisen (Bernstein & Lange, 2017). De veiligheid van internetbeveiliging loopt gevaar door de komst van quantumcomputers. Onderzoekers zijn in een race tegen de klok om nieuwe cryptografische technieken voor te bereiden vóór de komst van quantumcomputers. Lange en Bernstein analyseren in hun publicatie in Nature de mogelijkheden die beschikbaar zijn voor deze zogenaamde post-quantumcryptografie. Lange leidt een onderzoeksconsortium dat bestaat uit elf universiteiten en bedrijven om nieuwe cryptografische technieken te ontwikkelen. Informatiebeveiliging is uitgegroeid tot een onmisbare factor, vooral met moderne communicatienetwerken.

Door de technologische mogelijkheden die een quantum computer met zich meebrengt, leidt dit tot snellere rekenkracht, maar tegelijk brengt het ook nieuwe risico's met zich mee. Waar conventionele computers tijd nodig hadden om wachtwoorden te kraken, is dat probleem met de komst van een quantum computer opgelost. Een positief aspect is dat een quantum computer juist met behulp van verstrengeling de communicatie sterk genoeg kan maken dat het kraken hiervan nagenoeg onmogelijk wordt. Het is de TU Delft gelukt om twee elektronen met elkaar te verstrengelen die zich op ruim 1,2 km afstand van elkaar bevonden (Merali, 2015).

Dit is een relevante stap naar een onhackbaar internet waarmee informatie wordt verstuurd.

### *§3.4 Quantum computing en informatiebeveiliging*

In de huidige mondiale omgeving is het snel en veilig delen van informatie belangrijk om onze samenleving, de burgers, maatschappelijke en overheidsbelangen te beschermen. Sterke cryptografische algoritmes (cryptosystemen) en veilige protocolstandaarden zijn essentiële hulpmiddelen die bijdragen aan onze nationale veiligheid en helpen bij het aanpakken van de behoefte aan veilige, interoperabele communicatie (NSA, 2015). Cryptografie zit verborgen achter bijna alles wat digitaal gecommuniceerd wordt. Zo vormt het bijvoorbeeld een integraal onderdeel van internetstandaarden als TLS/ SSL, van digitale handtekeningen en van methoden voor het betrouwbaar opslaan van data in de cloud.

Zonder bescherming zal met behulp van quantumcomputers gevoelige informatie openbaar worden gemaakt, ook gegevens van jaren geleden. Dit kan leiden tot desastreuse datalekken. Een aanvaller kan onze beveiligde communicatie vandaag opnemen en jaren later breken met een quantum computer. Beredeneerd vanuit dat organisaties in toenemende maten digitaliseren, is dat bijna catastrofaal als het vanuit risico perspectief beredeneert voor vitale organisaties in de maatschappij zoals defensie, financiële instellingen en bedrijven in de zorgsector.

Organisaties zijn sterk aan het digitaliseren en met veel kracht en (gevoelige) data richting de cloud aan het bewegen. De cloud beschikt over enorm veel informatie en het moet worden voorkomen dat deze informatie in verkeerde handen valt, want dat zou een disruptief gevolg kunnen hebben, niet alleen op het bedrijfsleven maar ook op de samenleving. Daarom speelt dit ook een relevante rol in het kader van de nationale veiligheid. Alle geheimen van vandaag kunnen immers in verkeerde handen vallen, privégegevens, bank- en gezondheidsdossiers, maar ook staatsgeheimen. Hiervoor waarschuwt ook Tanja Lange, hoogleraar Cryptologie aan de Technische Universiteit Eindhoven. Zij houdt zich al sinds 2006 bezig met het belang van alternatieve systemen, en met de bewustwording en ontwikkeling van nieuwe systemen (Bernstein & Lange, 2017).

Daarnaast blijkt uit de kwetsbaarheidsanalyse spionage (KWAS) van de AIVD (AIVD, 2011) dat kennisname van informatie door een buitenlandse overheid de Nederlandse nationale veiligheid mogelijk kan aantasten en buitenlandse inlichtingdiensten en overheden er belang bij kunnen hebben deze informatie te bezitten. Het onderzoek laat zien dat in alle onderzochte sectoren kernbelangen zijn te vinden in de categorieën:

- Datasets en blauwdrukken: de in organisaties aanwezige gegevensbestanden, bouwtekeningen en ontwerpen;
- Standpunten en strategie: zoals beleidsstandpunten, onderhandelingsstrategieën en langjarige visies;
- Opkomende kernbelangen en infrastructuur: zoals wetenschappelijke innovaties die in de toekomst in concrete toepassingen belangrijke bijdragen aan de Nederlandse economie kunnen leveren.

## *§3.5 Informatiebeveiliging, interne beheersing en standaarden*

Ten tijde van het schrijven van deze scriptie bevinden we ons in de vierde industriële revolutie. Deze revolutie betreft de transitie van de industrie naar een digitale wereld waarin IT bijna alle aspecten van het productieproces heeft doordrongen. Het 'Internet of Things', het ontsluiten van informatie en het verbinden van gescheiden informatiestromen en productiestappen staan hierbij centraal. Daarnaast heeft COVID19 (Corona) dit proces alleen maar versneld. Gezien de snelheid van alle ontwikkelingen is het maar net de vraag of organisaties zich nu alleen moeten focussen op de eigen bedrijfsprocessen of dat sectoren zich moeten voorbereiden op een sectorgerichte aanpak en beheersing, waardoor niet alleen schaalvoordeel kan worden behaald, maar ook sectorbreed kan worden samengewerkt op verduurzaming en veiligheid. Organisaties zijn afhankelijk van IT. De dienstverlening van organisaties is in toenemende mate afhankelijk van meerdere (externe) partijen, waarbij die dienstverlening vaak ook afhankelijk is van IT. Dit roept ook de vraag op hoe organisaties om moeten gaan met de introductie van nieuwe technologieën (Leeuwen et al., 2015).

Conform de Wet Financieel Toezicht is DNB van oordeel dat financiële organisaties dienen te beschikken over adequate procedures en maatregelen ter beheersing van IT-

risico's. Ondernemingen hebben een verantwoordelijkheid om - de eigen omstandigheden in aanmerking nemende - op basis van een eigen analyse de juiste beheersing van IT risico's te ontwerpen en in te richten (DNB, 2021). De DNB heeft de afgelopen paar jaren veel aandacht besteed aan "Robuuste IT-systemen", echter ontbreken nu nog 'hands-on best practices' die gebruikt kunnen worden bij het "quantum veilig" maken van organisaties. Quantum-veilige cryptografie verwijst naar inspanningen om algoritmes te identificeren die bestand zijn tegen aanvallen van zowel klassieke als quantumcomputers, om informatie-assets veilig te houden, zelfs nadat een voldoende grote quantum computer is gebouwd.

Zonder quantum-veilig cryptografie en beveiliging is alle informatie die nu of in de toekomst via openbare kanalen wordt verzonden, kwetsbaar voor afluisteren (eavesdropping). Zelfs versleutelde gegevens die nu veilig zijn, kunnen worden opgeslagen voor latere ontsleuteling zodra er een praktische quantum computer beschikbaar komt. Tegelijkertijd zal het niet langer mogelijk zijn om de integriteit en authenticiteit van verzonden informatie te garanderen, aangezien datamanipulatie (data tampering) onopgemerkt blijft. Vanuit zakelijk, ethisch en juridisch oogpunt zou dit in strijd zijn met de huidige wettelijke vereisten voor gegevensprivacy en gegevensbeveiliging. Standaardisatie ten aanzien van het quantum-veilig worden is nog niet beschikbaar.

Om toch handvatten te hebben bij het quantum-veilig maken van processen is in deze scriptie ervoor gekozen om cryptografie te benaderen vanuit de dreiging en van daaruit te kijken naar bestaande standaarden die hierbij het beste passen. Literatuur over de aanpak van technologische bedreiggingen op processen leidt in eerste instantie tot de basisliteratuur over AO/IC. Starreveld schrijft over "bestuurlijke informatieverzorgingssystemen" en definieert bestuurlijke informatieverzorging als: "alle activiteiten met betrekking tot het systematisch verzamelen, vastleggen en verwerken van gegevens, gericht op het verstrekken van informatie ten behoeve van het besturen-in-engere-zin, het doen functioneren en het beheersen van een huishouding en ten behoeve van de verantwoordingen die daarover moeten worden afgelegd".

De organisatie wordt door Starreveld gezien als: “een systeem, een verzameling van componenten gegroepeerd bij een vorm van geregelde interactie om zodoende een organisatie als geheel te vormen. Een dynamisch (open) complex systeem dat zich kenmerkt door een proces dat invoer transformeert tot uitvoer en in belangrijke mate wordt beheerst door probabilistische relaties tussen de verschillende elementen en met de omgeving”. Starreveld verdeelt een informatieverzorgingssysteem onder in een informatiesysteem, de betrokken medewerkers, regelgeving, procedure, apparatuur en programmatuur. Het informatieverzorgingssysteem bestaat dus uit meer dan alleen het informatiesysteem (Starreveld & Leeuwen, 2002). Starreveld & Leeuwen onderscheiden binnen de bestuurlijke informatieverzorging vier objecten waarover een kwalitatief oordeel gegeven kan worden, te weten:

- De verstrekte informatie die aan haar doel moet beantwoorden;
- Het informatieverzorgingsproces als onderdeel van het desbetreffende systeem, dat kwalitatief verantwoorde informatie dient op te leveren;
- Het ontwerp- en ontwikkelingsproces dat het informatieverzorgingssysteem in casu als product heeft opgeleverd;
- De wijze waarop het beheer en het onderhoud van het informatieverzorgingssysteem in de organisatie zijn verankerd.

Starreveld gebruikt een vijfstappenplan dat ook gebruikt kan worden om gevolgen van IT-ontwikkelingen voor de administratieve organisatie en interne controle in kaart te brengen (Starreveld et al., 2002):

1. Stel kwaliteitseisen vast (exclusiviteit, integriteit/betrouwbaarheid, beschikbaarheid, beheersbaarheid, bescherming, controleerbaarheid);
2. Stel de bedreigingen vast;
3. Stel de risico’s vast;
4. Stel de beschikbare beheersmaatregelen vast;
5. Implementeer beheersmaatregelen.

Vanwege het tempo waarmee de technologische ontwikkelingen gepaard gaan, dient er nog een verdieping te worden gemaakt op de kwaliteitseisen van de beveiliging van data om cybersecurityrisico’s te voorkomen. Met de bovenstaande aspecten kan een eerste inventarisatie worden gemaakt om de volwassenheid van een quantum-veilig organisatie te meten. Naast een adequate interne beheersing vraagt

quantumtechnologie om een holistische visie op een wet- en regelgevend normenkader dat de belangen van de industrie in evenwicht brengt met die van de samenleving als geheel (European Commission, 2020). ENISA's post-quantum cryptography current state and quantum mitigation 2021 (ENISA, 2021) en NIST zijn standaarden op het gebied van cryptografische protocollen.

Doorbreking van cryptografie leidt in casu tot het risico van het mogelijk onderscheppen of uitlekken van gegevens, social engineering, ongeoorloofde toegang, het ongeoorloofd verkrijgen van rechten en ransomware, met als gevolg financiële- en reputatieschade. Voor een adequate interne beheersing zijn toereikende beheersmaatregelen nodig. De beheersmaatregelen ondersteunen de doelstellingen van de organisatie (Praat, 2018). Het is de verantwoordelijkheid van het management om toereikende beheersmaatregelen te treffen en ervoor zorg te dragen dat de beheersmaatregelen betrouwbaar (juist, tijdig en volledig) worden uitgevoerd (Praat, 2018).

Op basis van het voorgaande kan het begrip interne beheersing volgens Jan van Praat (Praat, 2018) als volgt worden gedefinieerd: "interne beheersing is het systeem van afspraken uitgevoerd door mensen op alle niveaus in een organisatie, dat gericht is op het verkrijgen van een redelijke mate van zekerheid omtrent het bereiken van doelstellingen in de volgende categorieën:
- Effectiviteit en efficiëntie van bedrijfsprocessen;
- Betrouwbaarheid van de informatieverzorging;
- Naleving wet– en regelgeving".

De informatie in de volgende tabel is deels gebaseerd op de categorisatie van de type maatregelen die organisaties dienen te nemen om de organisatiedoelstellingen te ondersteunen, zoals opgenomen in Interne beheersing gedefinieerd (Praat, 2018). Daarnaast is gebruik gemaakt van de door DNB opgenomen beheersmaatregelen, met betrekking tot deelgebieden van het totale spectrum van IT risico's, die relevant zijn voor ondernemingen (DNB, 2019-2020). De maatregelen zijn principle based en in casu gericht op risico's met betrekking tot informatiebeveiliging.

*Tabel 3: Beheersmaatregelen organisatie (Praat, 2018) aangevuld geplot uit DNB Good Practice (DNB, 2019-2020)*

| ***Type beheersmaatregel*** | ***Categorie*** | ***Beheersmaatregel DNB Good Practice (DNB, 2019-2020)*** |
|---|---|---|
| Organisatorische beheersmaatregelen | *Organization* | 5.1 Responsibility for risk, security and compliance<br>5.2 Management of information security<br>6.1 Data and system ownership<br>7.1 Segregation of duties |
| Procedurele beheersmaatregelen | *Governance* | 1.1 Information Security plan<br>1.2 IT Policies Management<br>2.1 Enterprise Information Architecture Model<br>2.2 Data classification scheme<br>3.1 Monitor future trends and regulations<br>3.2 Technology standards |
| | *People* | 8.1 Personnel recruitment and retention<br>8.2 Personnel competencies<br>8.3 Dependence upon individuals<br>8.4 Personnel clearance procedures<br>8.5 Job change and termination<br>9.1 Knowledge transfer to end users<br>9.2 Knowledge transfer to operations and support staff<br>9.3 Employee awareness |
| | *Process* | 10.1 Change standards and procedures<br>10.2 Impact assessment, prioritization and authorization<br>10.3 Test environment<br>10.4 Testing of changes<br>10.5 Promotion to Production<br>11.1 IT Continuity plans<br>11.2 Testing of the IT Continuity plan<br>11.3 Offsite backup storage<br>11.4 Backup and restoration<br>12.1 Storage and retention arrangements<br>12.2 Disposal<br>12.3 Security requirements for data management<br>13.1 Configuration repository and baseline<br>13.2 Identification and Maintenance of Configuration Items<br>15.1 Security incident definition<br>15.2 Incident escalation<br>16.1 Security testing, surveillance and monitoring<br>16.2 Monitoring of internal control framework<br>16.4 Evaluation of compliance with external requirements<br>16.5 Independent assurance<br>17.1 Identity Management<br>17.2 User account management |
| | *Outsourcing* | 14.1 Monitoring and reporting of SLA<br>14.2 Supplier risk management<br>16.3 Internal control at third parties |
| | *Risk management cycle* | 4.1 IT Risk Management framework<br>4.2 Risk assessment<br>4.3 Maintenance and monitoring of a risk action plan |
| Technische beheersmaatregelen | *Technology* | 18.1 Infrastructure resource protection and availability<br>18.2 Infrastructure maintenance<br>18.3 Cryptographic key management<br>18.4 Network Security<br>18.5 Exchange of sensitive data<br>19.1 Malicious software prevention, detection and correction<br>19.2 Vulnerability assessment<br>19.3 Application Life cycle management<br>20.1 Protection of security technology |
| | *Facilities* | 21.1 Physical security measures<br>21.2 Physical access |
| | *Testing* | 22.1 Penetration testing and ethical hacking |

Op basis van literatuurstudie dienen organisaties organisatorische, procedurele en technische maatregelen te treffen. DNB Good Practice beschrijft een lijst van beheersmaatregelen die organisaties kunnen hanteren om de wettelijke bepalingen ten aanzien van de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking te waarborgen. Voor de beheersing van cybersecurity risico's en risico's met betrekking tot informatiebeveiliging kunnen organisaties op basis van, de bedrijfsactiviteiten en organisatiestructuur, een risicoanalyse passende beheersmaatregelen treffen op grond van de aard, omvang en complexiteit van de risico's (DNB, 2019-2020).

Organisaties dienen zich bewust te zijn dat invoering van nieuwe cryptografische systemen van invloed is op de interne beheersing van organisaties. De implementatie van nieuwe cryptografische systemen gaat gepaard met organisatorische, procedurele en technische maatregelen (Praat, 2018). Praat beschrijft dat "goed veranderingsmanagement" hierbij van belang is.

Het niet beheersen van risico's met betrekking tot de doorbreking van cryptografie kan leiden tot blootstelling aan cyberaanvallen en reputationele schade en of verlies van vertrouwen vanuit de samenleving. Vanwege de complexiteit hanteert DNB Good Practice het kader van COBIT 4.1 (DNB 2019-2020). Deze beheersingsmaatregelen zijn niet alleen gericht op technologische oplossingen (Technology), zij zijn ook gericht op menselijk handelen (People), inrichting van processen (Processes) en faciliteiten, logische en fysieke toegangsbeveiliging tot informatie (Facilities). DNB hanteert een principle based kader met een continue cyclus, zoals het Plan, Do, Check, Act cyclus van ISO27001 (ISO27001, 2013). De afweging met betrekking tot de toepassing van het normenkader van DNB ligt bij de organisaties.

### *§3.6 Three Lines of Defense*

Waar het gaat over een ethische verantwoording speelt corporate governance een belangrijke rol. Voor het begrip corporate governance geeft de Preambule van de Corporate Governance Code in kernwoorden aan dat governance gaat over het besturen en beheersen, verantwoordelijkheid en zeggenschap en over toezicht en verantwoording. In de herziene Corporate Governance Code, principes 1.4.2 en 1.4.3

(https://www.mccg.nl/) staat opgenomen dat het bestuur van een organisatie in haar bestuursverslag informatie moet opnemen over een aantal elementen met betrekking tot de risicobeheersing. Dit betreft onder meer een expliciete verklaring, ook wel 'in-control statement' genoemd (ICS). Dit statement heeft betrekking op de werking van de interne controle- en risicobeheersingssystemen.

Eimers sprak al in 2008 over de volgende twee ontwikkelingen in de zakelijke omgeving:

- Globalisering en digitalisering
- Verbreding van transparantie en accountability

Internet werkt als drijvende kracht voor het structureren van de administratieve processen en zakelijke activiteiten. Digitalisering en globalisering dragen bij aan het Internet of Things (IoT), mondiaal opererende bedrijven en een meer netwerk-georiënteerde maatschappij (Eimers, 2008). Hij constateert dat het verlangen naar betrouwbare informatie op maatschappelijk niveau aanzienlijk is toegenomen. Gebruikers van die informatie steunen op de integriteit van de informatie die ze krijgen (Eimers, 2008). Hierbij stelt hij dat het de vraag is of de opstellers van die informatie dat waar kunnen maken. Eimers concludeert dat dit soort informatie om onafhankelijke verificatie vraagt (Eimers, 2008). Eimers verwijst naar een onderzoek van PWC en KPMG, KPMG heeft dit rapport in 2020 herijkt (PwC, 2008; KPMG, 2018; KPMG, 2020). Recent onderzoek bevestigt dat het vergroten van betrouwbaarheid (specifiek: geloofwaardigheid) de motivatie is waarom organisaties assurance bij rapportages relevant vinden. Vooral Globale trends, risico's, wet- en regelgevingen en reportingvereisten vragen steeds om meer betrouwbaarheid van informatie.

Ten aanzien van de rol van de accountant reflecteert Eimers op een aantal componenten uit de leer van het gewekte vertrouwen van Limperg (Limperg, 1932). "Inspelen op de behoeften van het maatschappelijk verkeer, niet meer verwachtingen te wekken dan je kunt waarmaken en het vertrouwen niet beschamen door je werk goed te doen – vergen in een veranderde omgeving ook een ander profiel van de accountant." Hierbij stelt Eimers: "Accountants moeten actiever de dialoog zoeken

met het maatschappelijk verkeer over hun behoeften aan zekerheid en op welke wijze de accountant hieraan invulling kan geven" (Eimers, 2008).

Eimers legt uit dat het relevant is dat een accountant cijfermatig bekwaam is, echter zorgt complexiteit voor een stijgende vraag naar breed georiënteerde accountants. Hierbij staan verbanden zien, inspelen op ontwikkelingen en oplossingen bieden voor de maatschappij centraal. Toekomstige accountants worden gezien als experts met kennis van informatietechnologieën, die een 'outside in'-blik kunnen bieden en in staat zijn om in multidisciplinaire teams samen te werken. Hierbij richt Eimers zich terecht ook op wat de invulling van de rol van het beroep wordt in nieuwe markten, waarbij hij concludeert dat de accountant oplettend moet zijn op ontwikkelingen die vragen om een onafhankelijke waardeoordeel. Teneinde toegevoegde waarde te kunnen blijven leveren aan de toenemende invloed van informatietechnologieën vraagt de controleaanpak om verbeteringen (Eimers, 2008).

Acties zodat accountants ook in de toekomst een rol van betekenis blijven spelen in het maatschappelijk verkeer (Eimers, 2008).


*Figuur 4: Herdrukt van ''De betekenis van de Accountant in een Dynamische wereld'' door Eimers, P. W. A., (2008), p.7. Vrije Universiteit.*

De producten waarbij accountants een belangrijke rol kunnen gaan spelen, vooral door de sterk toenemende ontwikkeling van Artificial Intelligence, big data, IoT en data-analyse, liggen op het vlak van continuous auditing en continuous assurance. Deze worden al decennia gezien als belangrijke toekomstige producten van accountants (Dassen, 2003). Elliot (2002) geeft een afbakening van deze twee termen:

- Continuous reporting: digitalisering van de informatie, alsmede van onmiddellijke beschikbaarheid via elektronische kanalen op het moment van het beschikbaar komen van de digitale informatie.
- Continuous assurance: een opdracht waarbij een accountant een conclusie formuleert die bedoeld is om de mate van vertrouwen die een beoogde gebruiker kan hebben over de beoordeling of meting van gedigitaliseerde informatie, dat wil zeggen de verantwoordelijkheid van een derde partij, tegen relevante criteria te vergroten, gelijktijdig met de totstandkoming van die informatie (Dassen, 2003).

Het uitgangspunt voor adequate controle en risicobeheersing is dat het eerstelijnsmanagement een eigen verantwoordelijkheid heeft op de executie van, de controle op en een adequate beheersing van haar eigen activiteiten. De tweede lijn staat opgesteld als adviesfunctie en adviseert over de richtlijnen en kaders. Daarnaast biedt de tweede lijn ondersteuning aan het eerstelijnsmanagement bij werkzaamheden op het gebied van controle en interne beheersing. De tweede lijn betreft onder andere risicomanagement-, compliance- en controllersfuncties.

De Interne Audit Functie (IAF) geeft een objectief oordeel over inefficiënties, overlappingen en gebreken in het risicobeheer. Het verstrekken van 'assurance' aan het topmanagement is de kerntaak van de IAF. Gramling et al. beschrijven mogelijke objecten van onderzoek (van de IAF). Governance, risicomanagement, internal controls, compliance en de betrouwbaarheid van de informatievoorziening dienen in opzet, bestaan en werking toereikend te zijn, zodat het management in staat is om gefundeerde besluiten te nemen (Gramling et al., 2004, p. 196; Institute of Internal Auditors, 2014, p. 4).

Resumé, op basis van literatuurstudie zijn verschillende perspectieven beschreven van de invloed van quantum computing op de informatiebeveiliging binnen organisaties. Enerzijds beïnvloedt quantum computing de informatiebeveiliging van organisaties door de doorontwikkeling van quantumcomputers met meer rekenkracht, ten opzichte van conventionele computers. Als baanbrekende quantumtechnologieën worden bijvoorbeeld quantum Artificial Intelligence en post-quantumcryptografische systemen genoemd. Anderzijds beschrijft de literatuur ook de potentiële dreigingen

die met deze ontwikkelingen gepaard gaan. Als belangrijk risico wordt de doorbreking van cryptografische systemen, met als gevolg blootstelling van kritieke en gevoelige data genoemd. Alsmede een aantal uitdagingen bij de verschillende toepassingen van quantum computing, onder meer de Europese privacywetten inzake datagebruik en gegevensverwerking, ook met betrekking tot kaderstelling en standaarden uit bescherming van (kritische) gevoelige (persoons)gegevens.

Praktische handvatten over hoe organisaties om moeten gaan met deze nieuwe technologieën lijken nog niet gestandaardiseerd. En de rol van de accountant en de IAF wordt vanuit de literatuur vooral onderkend in het verlenen van assurance en daarmee in de post-quantum situatie nog steeds als toegevoegde waarde gezien. Het management is vooral aan zet als het gaat om het implementeren van adequate interne beheersmaatregelen ten behoeve van de informatiebeveiliging van organisaties.
Het in hoofdstuk drie verantwoorde theoretisch kader is de basis voor het praktijkonderzoek. Op basis van een praktijkonderzoek (case study) wordt in Hoofdstuk 4 verder onderzocht of deze aannames in de praktijk worden onderkend.

# 4 Praktijkonderzoek (case study)

De volgende stap betreft een praktijkonderzoek op basis van reeds beschreven literatuur en interviews. De interviews zijn uitgevoerd op basis van de in Hoofdstuk 2.3 beschreven stappen 'prepare', 'collect' en 'analyze' van 'Case study research, design and methods', 4th edition (Yin, 2009).

Voor de praktijkanalyse worden tien virtuele interviews afgenomen, met experts binnen diverse organisaties in de sectoren: overheid, financiële dienstverlening, zorg en een wereldleider op de het gebied van quantumsoftware en quantumcybersecurity. De demografische gegevens zijn als volgt:

- vijf experts van organisaties uit verschillende sectoren (senior management, CISO of consultant), hierna te noemen organisaties;
- vijf experts van twee toonaangevende onderzoeksinstellingen op het vakgebied van quantum computing en technologie, hierna te noemen experts;
- met behulp van twee extra interviews met experts vindt er een kwaliteitscontrole plaats op de algehele gecodeerde resultaten uit de interviews.

Voor het praktijkonderzoek is als extra plausibiliteitscontrole gebruik gemaakt van enquêteresultaten en studierapporten van de volgende bronnen:

- Europese commissie Digital Economy and Society Index (DESI 2020);
- Enquête van Het Thales European Data Threat Report 2020 (Threat Report);
- Het Rapport van de Commissie toekomst accountancysector (2020).

De Europese commissie heeft verschillende studierapporten en analyses uitgebracht waarin onderzoek is gedaan naar Integratie van digitale technologie door ondernemingen, Cybersecurity en Nieuwe technologieën (Desi 2020).

Thales European Data Threat Report 2020 is een enquête onder 1.723 leidinggevenden op C-niveau, die verantwoordelijk zijn voor of invloed hebben op IT en informatiebeveiliging. De respondenten kwamen uit zestien landen, waaronder

Nederland. De organisaties vertegenwoordigen primair de gezondheidszorg, financiële diensten, detailhandel, technologie en federale overheid. De respondenten vertegenwoordigen organisatiegroottes, waarvan de meerderheid varieerde van 500 tot 10.000 medewerkers. Het onderzoek is uitgevoerd in november 2019.

Aan de hand van zeven interviewvragen wordt de praktijkanalyse, 'analyze' (Yin, 2009), van quantum computing en informatiebeveiliging binnen organisaties gepresenteerd. Daarna wordt onderzocht of de literatuurstudie op basis van de uitgevoerde praktijkanalyse wordt onderkend. Aan de hand van bestaande onderzoeksresultaten van het Threat Report, de Europese studierapporten (DESI) en het Rapport van de Commissie toekomst accountancysector (2020). worden de uitkomsten gecontroleerd op plausibiliteit.

De interviewvragen zijn gebaseerd op zeven open vraagstellingen waarop de ondervraagden moeten antwoorden:

1. Wat is jouw visie op quantum computing?

2. Wat zijn de kansen en bedreigingen van Quantum computing en in het licht van cryptografie?

3. Op welke manier beïnvloedt Quantum computing de informatiebeveiliging in bedrijfsprocessen?

4. Hoe verschilt de implementatie van post-quantumcryptografie ten opzichte van veel toegepaste cryptografische methoden?

5. Zijn er algemeen aanvaardbare standaarden voor de toepassing van Quantum computing? En wat moet de belangrijkste focus zijn van toekomstige normen?

6. Wat is de rol van accountants / IT - auditors op dit gebied?

7. Wat is jouw visie op of er voldoende bewustzijn is bij organisaties met betrekking tot de kansen en bedreigingen van quantum computing?

## *§4.1 Analyse*

Aan de hand van zeven interviewvragen is een beeld gevormd over quantum computing en informatiebeveiliging binnen organisaties. Op basis van de afgenomen interviews zijn de resultaten open, axiaal en selectief gecodeerd en is een antwoord geformuleerd op de vraagstellingen. De hoofdlijnen zijn opgenomen in een matrix. De uitkomsten zijn hieronder opgenomen. Als plausibiliteitscontrole is gebruik gemaakt van de enquêteresultaten en studierapporten van DESI 2020, Threat Report en het Rapport van de Commissie toekomst accountancysector (2020).

### Vraagstelling 1

Ten aanzien van vraagstelling 1 hebben de ondervraagden per sector een andere mening. De ondervraagde experts zijn het erover eens dat het een kwestie van tijd is voordat de quantum computer sterk genoeg is om veelgebruikte cryptografische systemen te doorbreken[3]. Van de tien interviews noemen alle ondervraagden de voorspellende eigenschappen, (quantum Artificial Intelligence), het optimaliseren van processen en quantum communicatie als voordelen en het doorbreken van cryptografieën als nadeel.

Van de ondervraagde organisaties is de meerderheid, vier van de vijf organisaties, sceptisch over wanneer de eerste quantum computer sterk genoegd is om cryptografieën te doorbeken. Zij verwachten dat dit niet op korte termijn zal gebeuren.

Alle ondervraagde experts zijn allen hier minder sceptisch over en kijken vooral naar de exponentiële ontwikkeling van de huidige quantumcomputers, waarbij niet alleen het aantal qbits, maar ook een lagere error rate van belang is voor een exponentiële toename in computingkracht dat nodig is voor het doorbreken van veelgebruikte cryptografie. Alle ondervraagde experts uit het interview hebben aangegeven dat het een misvatting is als organisaties mogelijk pas bij het evident zijn van een quantum computer actie gaan ondernemen. Organisaties moeten volgens experts tijdig beginnen met de migratie naar quantum-veilige cryptografie.

Vraagstelling 2

Ten aanzien van vraagstelling 2 noemen alle ondervraagden het doorbreken van cryptografie en onderscheppen van gevoelige data als dreiging. Drie van de tien ondervraagden noemen QKD als kans. Drie van de tien ondervraagden noemen quantumcryptografie (verstrengeling) als kans. Twee van de tien ondervraagden noemen quantum computing als kans. Één ondervraagde noemt het kunnen stimuleren van quantum systemen en daarmee de toepassing van nieuwe medicijnen en materialen als kans. Één ondervraagde noemt de analysemogelijkheden als kans.

*Deze uitkomsten zijn ook in lijn met DESI - Emerging Technologies 2020, (DESI 2020). Quantum computing kan in veel sectoren worden toegepast (bv. Lucht- en ruimtevaart, landbouw, gezondheid, productie, automobiel of energie) en in combinatie met andere digitale technologieën. Geavanceerde cryptografietechnieken kunnen bijvoorbeeld helpen bij het ontwikkelen van veilige communicatie en het detecteren van netwerkinbraken.*

Acht van de tien ondervraagden zijn van mening dat organisaties zich nog in een conceptuele fase bevinden. Ondervraagden geven aan dat organisaties nog niet bezig zijn met het treffen van voorbereidingen dan wel het in kaart brengen van de scope en risico's. Alle ondervraagden geven aan dat organisaties vooral nog bezig zijn met begripsvorming, ook ten aanzien van mogelijke toepassingen, kansen en dreigingen.

NB. Bij het uitvoeren van de kwaliteitscontrole is naar voren gekomen dat het algoritme van QKD situationeel hackbaar is (Makarov et al., 2018).

Vraagstelling 2 – 3 – 4

Uit de nadere analyse van de antwoorden op de vraagstellingen 2, 3 en 4 blijkt dat drie van de vijf ondervraagde organisaties één voorbeeld konden gegeven van cryptografie dat niet meer veilig is bij de komst van een quantum computer. Ondervraagde organisaties hebben aangegeven dat er behoefte is aan meer informatie en guidence over veilige cryptografie.

Vijf van de tien experts verwijzen naar het quantum-veilig maken van de IT-architectuur en NIST als voorloper op post-quantumcryptografie.

*Deze uitkomsten zijn ook in lijn met de enquêteresultaten van het Thales European Data Threat Report 2020 (Thales, 2020). Thales 2020 vermeldt dat volgens de ondervraagde organisaties de belangrijkste strategieën om quantum computingbedreigingen te compenseren, veranderingen in de IT- / beveiligingsarchitectuur zijn (35%) en key management infrastructuur deployment (34%). Maar veel organisaties zijn onzeker over hoe ze zouden moeten reageren.*

Tabel 6 toont verschillende type algoritmes[3]. De rood gearceerde algoritmes moeten door organisaties tijdig worden vervangen, omdat deze algoritmes doorbroken kunnen worden met het algoritme van Grover of met het algoritme van Shor op een (voldoende grote) quantum computer.

| Type | Algoritme | Key lengte | Conventionele computer | Quantum computer |
|---|---|---|---|---|
| Symmetrisch | AES-128 | 128bits | 128 bits | 64 bits * |
| Symmetrisch | AES-256 | 256bits | 256 bits | 128 bits |
| Asymmetrisch | RSA-1024 | 1024 bits | 80 bits | 0 bits |
| Asymmetrisch | RSA-2048 | 2048 bits | 112 bits | 0 bits |
| Asymmetrisch | ECC-256 | 256 bits | 128 bits | 0 bits |
| Asymmetrisch | ECC-384 | 384 bits | 192 bits | 0 bits |
| Asymmetrisch | ECDSH-256 | 256 bits | 128 bits | 0 bits |
| Hash | SHA-2 | 256 bits | 128 bits | 85 bits |
| Hash | SHA-2 | 384 bits | 192 bits | 128 bits |

*Tabel 4: Algoritmes tegen aanvallers met conventionele computers en aanvallers met een quantum computer (Muller & Van Heesch, 2020).*

**Er zijn verschillende uitdagingen die moeten worden overwonnen voordat quantumcomputers symmetrische cijfers zoals AES-128 te doorbreken. Rekening houdend met deze uitdagingen is een alternatieve opvatting dat AES-128 de komende decennia veilig zal blijven (NIST).*

Uit de nadere analyse van de antwoorden op de vraagstellingen 2, 3 en 4 blijkt dat organisaties grote hoeveelheden (gevoelige) data bezitten. Deze zijn vaak nog ongestructureerd. Ondervraagden willen data op een efficiënte manier kunnen ontsluiten om van nieuwe technologisch gedreven toepassingen gebruik te kunnen maken. Van de ondervraagden zijn alle ondervraagden het erover eens dat om te kunnen optimaliseren, organisaties in toenemende mate datagedreven worden. Daarom ziet een meerderheid van de ondervraagden de optimalisatiemogelijkheden

[3] Herdrukt van ''Migration to quantum-safe cryptography'', door TNO, 2019. Position paper, p.13.

van een quantum computer als kans. De meerderheid van de ondervraagden geven aan dat door de sterke mate van digitalisering en de behoefte van organisaties aan een robuust en wendbaar IT-landschap, organisaties in toenemende mate hun data in de cloud plaatsen. Daardoor zijn alle ondervraagden het met elkaar erover eens dat door deze beweging de blootstelling van data groter wordt dan alleen de perimeter van het traditionele IT-landschap en dus kwetsbaarder voor cyberaanvallen.
Organisaties noemen het kritisch kijken naar het shared responsibility model een belangrijk element. Daarnaast geeft een meerderheid van de ondervraagden aan dat er nog onvoldoende kennis, geld en resources beschikbaar zijn omtrent datagericht beveiligen.

*Deze uitkomsten zijn ook in lijn met de enquêteresultaten van het Thales European Data Threat Report 2020 (Thales 2020). Thales 2020 vermeldt dat 48 % van alle data dat door de onderzochte organisaties in de cloud wordt opgeslagen gevoelige data is. Doordat meer gevoelige gegevens in de cloud worden opgeslagen nemen de beveiligingsrisico's toe. Dit is in lijn met de observaties van DESI – Cybersecurity, (DESI 2020).*

*De meerderheid van de in de survey betrokken organisaties percipiëren de verantwoordelijkheden die hierbij horen anders dan de cloud providers.*
*Van alle respondenten geeft 34% aan een focus te hebben op data security en data security gemiddeld 15% van het IT-budget omvat.*

*De focus op de beveiliging ook buiten de perimeter om off-premises gegevens te beschermen dient verder te worden verbeterd. Van de respondenten zegt 100% dat ten minste een deel van hun gevoelige gegevens in de cloud niet is versleuteld.*

Van de ondervraagden hebben vijf van de vijf ondervraagde organisaties geen beeld bij hoe post- quantumcryptografie eruitziet. Hierbij zijn vijf van de tien interviews niet meegeteld omdat dit wetenschappelijke onderzoeksinstellingen of experts zijn die als expert in het vakgebied worden beschouwd. Door de experts wordt quantum-veilige cryptografie onderverdeeld in de volgende twee categorieën:

1. Quantumcryptografie: Het belangrijkste voorbeeld in deze categorie is Quantum Key Distribution (QKD) (NCSC, 2020).

2. Post-quantumcryptografie: de studie van "conventionele" cryptografische algoritmes, dat wil zeggen algoritmes die niet gebaseerd zijn op quantummechanica, waarvan wordt aangenomen dat ze beveiligd zijn tegen aanvallen door een quantum computer (Muller & Van Heesch, 2020).

*Deze uitkomsten zijn ook in lijn met de enquêteresultaten van het Thales European Data Threat Report 2020 (Thales 2020). Thales 2020 vermeldt dat uit de enquête blijkt dat slechts 57% van de opgeslagen gevoelige gegevens in de cloud wordt beschermd door encryptie. De ondervraagden geven hiermee aan dat minstens een deel van de in de cloud opgeslagen gevoelige gegevens niet versleuteld zijn.*

Vraagstelling 3 – 4

Ten aanzien van vraagstelling 3 maken alle ondervraagden zich zorgen over het geheim blijven van gevoelige data.

De ondervraagde experts geven aan dat het moment nu is om binnen organisaties actie te ondernemen voor het quantum-veilig maken van de infrastructuur en hoe langer hiermee gewacht wordt het risico groter wordt dat gevoelige data niet meer veilig is. Experts benadrukken crypto-agility (flexibiliteit in cryptografische algoritmen en sleutellengten). Anders is het voor een aanvaller mogelijk om eerder onderschepte communicatie met terugwerkende kracht te ontcijferen.

Ten aanzien van vraagstelling 4 hebben drie van de vijf organisaties geen beeld bij hoe de implementatie van post-quantumcryptografie ten opzichte van veel toegepaste cryptografische methoden verschilt. Twee van de vijf organisaties hebben in hoofdlijnen een beeld van hoe post-quantum cryptografische methodes verschillen. Hierbij wordt met name de nadruk gelegd op dat er cryptografie bestaat dat veilig geacht wordt, maar de aanpak kan niet expliciet worden gemaakt.

Experts geven aan dat van post-quantum cryptografie aangenomen wordt dat deze veilig is tegen quantum computers. En verwijzen daarbij naar onder meer NIST (Moody et al., 2020) en ENISA (ENISA, 2021).

*Deze uitkomsten zijn ook in lijn met de enquêteresultaten van het Thales European Data Threat Report 2020 (Thales 2020). Thales 2020 vermeldt dat ruim 70% van alle respondenten uit verschillende sectoren (overheid, zorg en financiële dienstverlening) verwacht dat quantumcryptografie impact zal hebben op hun organisatie. Binnen deze sectoren maakt 92% van de overheidsorganisaties zich zorgen over exposure van gevoelige data, gevolgd door 88% van de organisaties binnen de zorgsector en 77% binnen de financiële dienstverlening.*

Uit de afgenomen interviews met de experts en standaarden zoals de NISTIR 8105 blijkt dat de implementatie van cryptografie-infrastructuur met public keys bijna twintig jaar heeft geduurd. Daarom vergt het een aanzienlijke inspanning om een veilige migratie van de huidige veelgebruikte cryptosystemen naar quantum-veilige cryptosystemen te garanderen (Chen et al., 2016).

Vraagstelling 5

Ten aanzien van vraagstelling 5 hebben drie van de vijf ondervraagde organisaties geen beeld bij welke standaarden en of normen geraadpleegd kunnen worden.
Vijf van de vijf organisaties hebben behoefte aan een best practise.

Van de tien ondervraagden verwijzen zeven naar NIST. Het rapport van NIST, NISTIR 8105, onderbouwt dat symmetrische algoritmes en hashfuncties bruikbaar zijn in een quantumtijdperk (Chen et al.,2016). Omdat deze algoritmes resistent zijn tegen aanvallen van zowel klassieke als quantumcomputers zijn standaarden gericht op algoritmes met public keys (ETSI 2015, & Perlner et al., 2009).

De ondervraagde experts adviseren drie belangrijke stappen die organisaties nu al kunnen nemen:

1. Organisaties moeten bepalen hoelang (gevoelige en geheime) informatie geheim moet blijven. In het bijzonder bij een harvest-now-decrypt-later-aanval wordt de informatie nog steeds gecompromitteerd.
2. Inventariseren welke type cryptografie waar wordt toegepast in voorbereiding op de migratie naar quantum-veilige cryptografie.

## Vraagstelling 6

Van alle ondervraagden zien zes van de tien ondervraagden niet direct een rol weggelegd voor de accountant/IT Auditor.

Vier van de vijf ondervraagde organisaties hebben behoefte aan specialistische kennis over quantum-veilige cryptografie.

De ondervraagden benadrukken dat een accountant/IT auditor vanuit zijn rol van toegevoegde waarde kan zijn bij het geven van een onafhankelijk oordeel over informatiemanagementsystemen en informatiebeveiligingssystemen.

Één ondervraagde heeft ook meer behoefte aan een IAF die in de beoordeling ook rekening houdt met technologische ontwikkelingen versus de door het management opgestelde strategische IT en domein-architectuur. Aldus een meer prospectieve benadering dan retrospectieve benadering. Alle experts geven aan dat het relevant is dat organisaties voor zichzelf een actieplan maken waarin zij ook inventariseren of ze de benodigde kennis in huis hebben.

*Dit is in lijn met het Rapport van de Commissie toekomst accountancysector (2020). Technologische ontwikkelingen zullen naar verwachting een niet onbelangrijke impact hebben op accountants en hun werk. De kans is aanwezig dat er in de toekomst minder behoefte zal zijn aan omvangrijke controleteams bestaande uit accountants met oplopende ervaring in het beroep. Het is zeer wel denkbaar dat samenstelling van die controleteams zal veranderen en specialisten, Data Analysts of Information Security Analysts, een relevante rol gaan spelen.*

## Vraagstelling 7

Ten aanzien van vraagstelling 7 verwachten vier van de vijf ondervraagde organisaties dat het onderwerp pas hoog op de agenda komt te staan op het moment dat de ontwikkeling van een quantum computer zover is dat deze cryptografie kan doorbreken. Een aantal quotes uit alle interviews die het gezamenlijke beeld versterken:

- *"Harvest now decrypt later."*

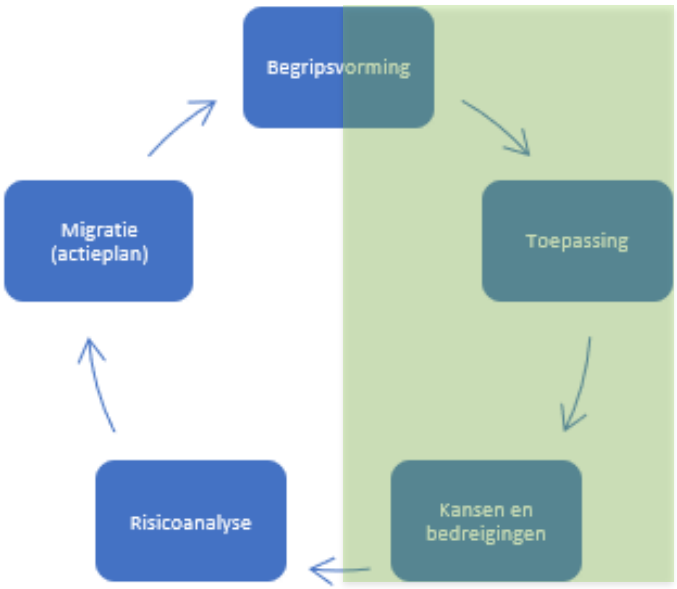
- *"Het is een ver-van-mijn-bed-show."*
- *"Organisaties kijken nog de kat uit de boom."*

## *§4.2 Resultaat*

De resultaten van het praktijkonderzoek zijn geplot in twee figuren die de huidige situatie weergeven. Daarnaast wordt teruggegrepen op de geformuleerde deelvragen. Eventuele aannames worden verklaard, resultaten worden vergeleken met de literatuur en beperkingen worden toegelicht.

***Kansen en bedreigingen van quantum computing***

Figuur 5 is opgesteld op basis van de resultaten van het praktijkonderzoek en is een eigen grafische weergave van de (risico)volwassenheid, met betrekking tot de randvoorwaarden die nodig zijn voor een transitie naar een quantum-veilige situatie. Organisaties bevinden zich nog vooral in het groene gebied.




*Figuur 5: Grafische weergave van de (risico)volwassenheid van organisaties met betrekking tot quantum computing.*

Een meerderheid van de ondervraagde organisaties zijn nog bezig met begripsvorming van quantum computing, de toepassingen en kansen en bedreigingen. Organisaties zijn nog niet gestart met een risicoanalyse en een actieplan. Naast tijd,

geld, resources en complexiteit wordt aangedragen dat dit onderwerp nog in een vroeg stadium zit en nog weinig aandacht krijgt op de bestuurstafel.
Daarnaast ondervinden organisaties uitdagingen zoals benoemd in Figuur 6. Er wordt nog niet geïnvesteerd in kennis, competenties op het gebied van quantum computing. Wel neemt een meerderheid van de ondervraagden deel aan gremia waarin cyberdreigingen en cyberaanvallen worden gedeeld. Één van de organisaties merkt ook op in hoeverre de huidige cyber security maatregelen ook in staat zijn om doorbreking van cryptografie te herkennen. In lijn met de literatuurstudie en opinie van experts is het daarom relevant dat organisaties tijdig beginnen met de migratie naar quantum-veilige oplossingen. Experts benadrukken dat een migratie een lange doorlooptijd heeft.

De ondervraagde organisaties zijn nog niet bezig met de implementatie van post-quantumcryptografie. Uit een detailanalyse blijkt dat een meerderheid van de organisaties nog een afwachtende houding hebben en sceptisch zijn over de snelheid waarmee een quantum computer wordt ontwikkeld. In tegenstelling tot experts die juist de nadruk leggen op de voorbereidingen die nu getroffen moeten worden.
Alle ondervraagden zijn het eens met elkaar eens over dat een quantum computer er gaat komen en deze ook in staat is cryptografie te doorbreken. Uit interviews blijkt dat voor de ondervraagde organisaties de tijdshorizon nog onduidelijk is. Daarnaast is er een behoefte aan meer praktische kennis om te weten wanneer, welke stappen moeten worden genomen om eventuele risico's, die met de komst van een quantum computer ontstaan, te vermijden. Er is een behoefte aan standaardisatie en best practises die kunnen helpen bij een migratie naar een post-quantumcryptografie. De meeste experts zijn het erover eens dat quantumcomputers waarschijnlijk binnen 10 tot 20 jaar werkelijkheid worden (Mosca et al., 2021) & (AIVD, 2015).

Uit interviews met experts blijkt dat over de kracht/kansen van quantumcomputers misvattingen bestaan. Het is een aanname dat quantumcomputers direct oplossingen leveren voor willekeurige rekenproblemen. Dit is niet het geval, omdat de werkelijke kracht van een quantum computer beperkt is tot specifieke algoritmes en alleen verbetering biedt voor een beperkt aantal toepassingen. Naast optimalisatie van processen (quantum Artificial Intelligence) is cryptoanalyse één van deze toepassingen. Om als organisatie hiervan te kunnen profiteren moeten organisaties

eerst nadenken welke optimalisatieprobleem ze zouden willen oplossen. Omdat de toepassing gebaseerd is op algoritmes heeft een organisatie wiskundigen nodig die deze optimalisatieprobleem kunnen operationaliseren in een algoritme. Dit soort kennis is specialistisch, daarom is het belangrijk dat organisaties op tijd beginnen en inventariseren welke kennis en expertise zij nodig hebben.

Voor organisaties wegen op korte termijn de nadelen zwaarder op dan tegen de voordelen, omdat de impact van een quantum computer op het gebied van beveiligde communicatie ernstig is. Het door een voldoende grote quantum computer kunnen doorbreken van cryptografie leidt ook tot het kunnen onderscheppen van (gevoelige) bedrijfsinformatie dan wel staatsgeheimen. Daarom vormen quantum computers een zeer ernstige bedreiging voor veel gebruikte cryptosystemen.

De uitkomsten zijn in lijn met de plausibiliteitscontrole en met de literatuurstudie. Quantum computing is een complex onderwerp dat in de praktijk deze uitdagingen kent. Hierbij zijn organisaties nog zoekende in het wanneer-wie-wat en hoe actie moet worden ondernomen. Uit het praktijkonderzoek blijkt dat organisaties achter lopen op de ontwikkelingen die in het literatuuronderzoek naar voren komen. Uit literatuuronderzoek blijkt dat organisaties nu al voorbereidingen moeten treffen in aanloop naar de implementatie van post-quantumcryptografie. Dit wordt ook onderkend door de geïnterviewde experts.

***De implementatie van post-quantum cryptografie op conventionele computers ten opzichte van andere, veel toegepaste cryptografische methoden***

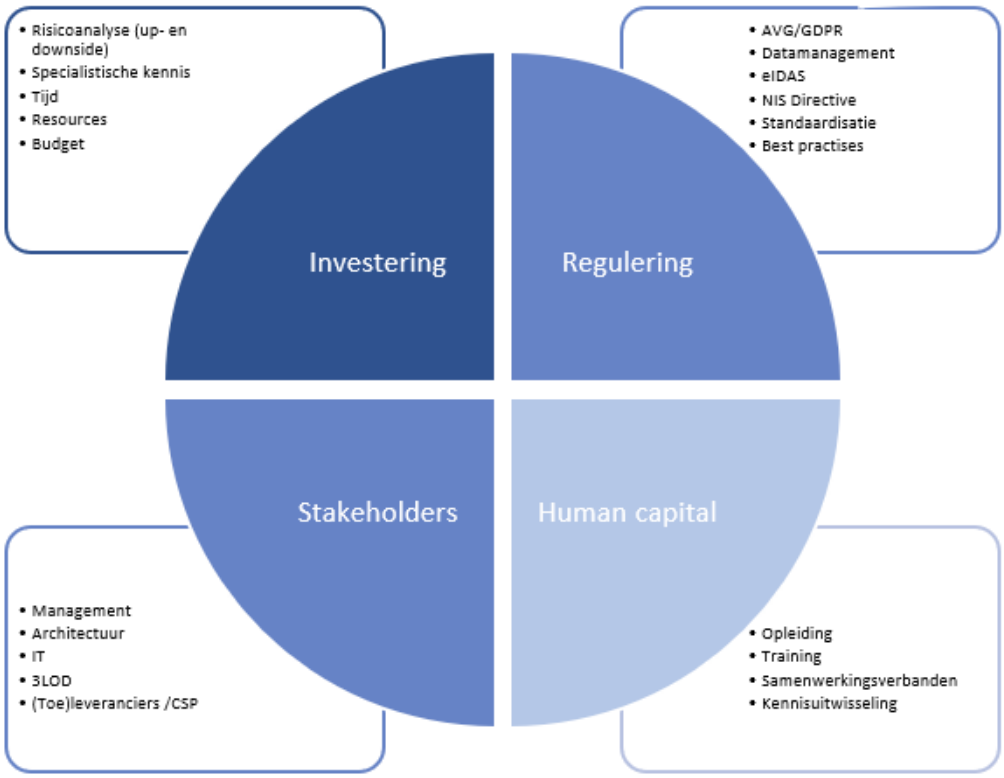
Uit zowel literatuurstudie als interviews met experts wordt duidelijk dat key exchange (sleuteluitwisseling) en symmetrische versleuteling tegen quantum computers beveiligd moeten zijn, lang voordat de quantum computers evident zijn. Anders is het voor een aanvaller mogelijk om eerder onderschepte communicatie met terugwerkende kracht te ontcijferen: “harvest now, decrypt later”. Certificaten en digitale handtekeningen die in de verre toekomst vervallen, moeten worden beveiligd tegen aanvallen met quantum computers. Hiervoor is het belangrijk protocollen en updatemechanismen te gebruiken die het upgraden naar een quantum-veilige cryptografie mogelijk maken zodra deze beschikbaar zijn.

Op basis van literatuurstudie en interviews met experts wordt geadviseerd om versleutelde gegevens die lange tijd vertrouwelijk moeten zijn opnieuw te versleutelen met quantum-veilige oplossingen. Experts adviseren om rekening te houden met de vraag of het verwijderen van de niet-quantum-veilige versleuteling voorafgaand aan het toepassen van de quantum-veilige versleuteling onaanvaardbaar kan zijn, omdat gedurende de tijd dat de gegevens onbeschermd zijn, deze kunnen worden aangetast. Als de gegevens niet langer actief nodig zijn, maar vertrouwelijk moeten blijven, moeten ze in quarantaine worden geplaatst, dat wil zeggen offline worden gehaald en op een fysiek beschermde locatie worden opgeslagen.

De ondervraagde organisaties zien vooral de dreiging en het gevolg en zijn ten tijde van het schrijven van deze scriptie minder bezig met de oplossingen. De ondervraagde organisaties zitten vooral nog in een conceptuele fase. De technologische assessment, implicaties en acties zijn nog niet in kaart gebracht.

***Invloed van quantum computing op informatiebeveiliging in bedrijfsprocessen***

Uit het praktijkonderzoek blijkt dat alle ondervraagden in de kern vier uitdagingen zien in de huidige situatie ten aanzien van quantum computing en informatiebeveiliging binnen organisaties. Figuur 5 is opgesteld op basis van de afgenomen interviews en betreft een eigen grafische weergave van de uitdagingen, geplot in vier deelgebieden, die worden onderverdeeld in een aantal onderliggende aandachtpunten.




*Figuur 6: Grafische weergave van de uitdagingen voor organisaties in de huidige situatie bij een migratie naar een quantum-veilige organisatie.*

Uit de analyse blijkt dat vier van de vijf ondervraagde organisaties zich in de rechterflank van Figuur 6 bevinden. Uit interviews blijkt dat organisaties niet direct inzicht hebben in welke type cryptografie waar wordt toegepast. Organisaties zijn wel op de hoogte van het risico dat een quantum computer veelgebruikte cryptografieën kan doorbreken. Echter zijn organisaties nog niet zo ver dat ze dit inzicht en overzicht hebben, ofwel de risicoanalyse en actieplan is nog niet gemaakt.
Voor de experts is dit herkenbaar. De fase waarin de ondervraagde organisaties zich bevinden staan haaks op het standpunt van experts en NISTIR 8105 (Chen et al.,2016) en (ETSI 2015, & Perlner et al., 2009). Twee aspecten zijn randvoorwaardelijk om als organisatie de impact van quantum computing op de informatiebeveiliging beheersbaar te houden:

- Een tijdige beschikbaarheid van quantum-veilige asymmetrische, gestandaardiseerde algoritmes om te kunnen migreren. Als deze niet tijdig beschikbaar zijn, kan dit leiden tot zwakke punten in het algoritme en/of fouten in de implementatie.
- Een tijdige afronding van de migratie. Indien dit niet mogelijk is, moeten mitigerende maatregelen worden genomen om de risico's op een andere

manier te mitigeren, bijvoorbeeld door, risico gebaseerd, gegevens in quarantaine te plaatsen en of een verzekering af te sluiten

Ook de Amerikaanse inlichtingendienst, National Security Agency (NSA) raadt op haar website organisaties aan om vooral nu te starten met het treffen van voorbereidingen op een quantum-veilige algoritme- overgang. Dit is waarom, ongeacht de exacte tijd van de komst van het quantumcomputertijdperk, nu begonnen moet worden met het voorbereiden van de informatiebeveiligingssystemen om quantumcomputers te kunnen weerstaan.

Op basis van literatuuronderzoek en het standpunt van experts moeten algoritmes door organisaties tijdig worden vervangen, omdat deze algoritmes doorbroken kunnen worden met het algoritme van Grover of met het algoritme van Shor op een (voldoende grote) quantumcomputer. Het is belangrijk om alle technische maatregelen en elementen van certificaten, digitale handtekeningen en sleutelbeheer bij te werken naar quantum-veilige opties. Good practises en of best practices ten aanzien van een transitie naar een quantum-veilige cryptografie is ten tijde van het schrijven van deze scriptie nog niet beschikbaar. Wel kunnen organisaties starten met een inventarisatie van de gebruikte cryptografische oplossingen. Experts geven aan dat nu al begonnen moet worden met een Plan, Do en Check om te voorkomen dat organisaties achterlopen op de technologische ontwikkelingen op het gebied van quantum computing en de risico's ervan. De ondervraagde organisaties geven in beginsel ook aan geen inzicht te hebben in waar welke type cryptografische oplossingen binnen organisaties gebruikt worden.

***Algemeen aanvaardbare standaarden voor de toepassing van quantum computing***

NISTIR 8105, suggereert wel dat symmetrische algoritmes en hash-functies bruikbaar zijn in een quantumtijdperk (Chen et al.,2016). Omdat deze algoritmes resistent zijn tegen aanvallen van zowel klassieke als quantumcomputers, zijn standaarden gericht op algoritmes met public keys (ETSI 2015, & Perlner et al., 2009). NIST merkt wel op dat voor geen van de resistente post-quantumcryptografie voorstellen is aangetoond dat het de veiligheid tegen alle quantumaanvallen garandeert. Dit betekent dat een nieuw quantumalgoritme kan worden ontdekt dat sommige van deze ''veilige'' schema's doorbreekt. Dit is echter vergelijkbaar met de huidige

cryptografie. Het ontbreken van bekende aanvallen wordt gebruikt om de beveiliging van de huidige cryptografie met openbare sleutels te rechtvaardigen.
Om quantum-veilige algoritmes te kunnen implementeren werken momenteel verschillende standaardisatie-instellingen aan standaardisatie van post-quantumcryptografie (Muller & Van Heesch, 2020).

Ten tijde van het schrijven van deze scriptie zijn er nog geen goedgekeurde algemeen aanvaardbare normen gestandaardiseerd. NIST is wel hiermee bezig en voor zover bekend is NIST hierin voorloper. De eerste conceptnormen van NIST zullen naar verwachting tussen 2022 en 2024 beschikbaar komen (Muller & Van Heesch, 2020). Dit wordt ook onderkend door de geïnterviewde experts. Alle organisaties zitten nog in de aanloopfase, NIST wordt door de meerderheid genoemd als mogelijke standaard. Dit is in lijn met de literatuurstudie. Experts wijzen er ook op dat het doel van gegevensbescherming moet worden bereikt conform EU wet- en regelgeving inzake dataprotectie en de beveiliging van netwerk- en informatiesystemen bijvoorbeeld NIS (NIS Directive, 2020). Deze wetten specificeren niet welke specifieke technische procedures, cryptografische schema's of parameters moeten worden geïmplementeerd, maar dicteren dat het doel van gegevensbescherming moet worden bereikt.

***De rol van de auditprofessie***

De rol van de accountant en de IAF is op basis van de interviews vooral van toegevoegde waarde op het gebied van assurance en als trusted advisor van het management. Vanuit de literatuurstudie is de positionering van de interne audit functie (IAF) onderdeel van het three lines of defence model. Uit het literatuuronderzoek blijkt dat de scope in het audituniversum afhankelijk is van de processen, projecten en IT-systemen van een organisatie en daarmee ook van de strategie, doelstellingen en risicobereidheid van de organisatie. Dit is in lijn met de uitkomsten van de interviews. Organisaties (uitgezonderd experts in het vakgebied) zijn hier nog niet veel mee bezig omdat het nog geen onderdeel is van de strategische (IT) doelstellingen van de organisatie.
Dit is in lijn met het literatuuronderzoek. Wallage en Van Leeuwen (2017) stellen dat de functie van de IAF gebonden is aan de omvang, aard, complexiteit en besturingsfilosofie van de organisatie. Voor de externe accountant geldt dat volgens

het Rapport van de Commissie toekomst accountancysector (2020), het accountantsberoep door technologische ontwikkelingen zal veranderen. Door de toepassing van nieuwe technologie zal door innovatie de kwaliteit van de controles toenemen. Daarnaast noemt het rapport dat het beroep meer IT gedreven wordt, maar er aanzienlijk minder behoefte zal zijn aan accountants zoals we die nu kennen.

# 5 Conclusie

Op basis van verschillende interviews met experts uit het vakgebied, literatuuronderzoek en onderbouwende standaarden zoals NIST (Moody, et al., 2020), ETSI (ETSI, 2015) en ENISA (ENISA, 2021) is het duidelijk dat quantum computing van invloed gaat zijn op de informatiebeheersing van organisaties. De applicaties die hieraan ten grondslag liggen steunen op de veiligheid van de communicatie, bijvoorbeeld op de authenticiteit, privacy, dataprotectie en integriteit. Het gaat om vertrouwen. Deze veiligheidsvoorwaarden houden de informatiebeveiligingsprocessen beheersbaar en worden mogelijk gemaakt door het gebruik van cryptografie. Er zijn verschillende stappen nodig om de IT-infrastructuur van organisaties voor te bereiden op de komst van een voldoende grote quantum computer:

- Bepalen van de scope van cryptografie die door een organisatie wordt gebruikt (neem (onder)leveranciers mee in deze scope). Alle soft- en hardware-assets (inclusief data) die cryptografie gebruiken, zie Figuur 7 bijlage 3.
- Plan van aanpak voor de bijwerken van de gebruikte cryptografie en hash-functies die te zwak zijn om een quantum computer te weerstaan. Overzicht en inzicht in alle versleutelde en of ondertekende data en de lengte in jaren die de versleuteling nodig heeft om intact te blijven of dat de handtekening geldig moet blijven:
    - Organisatie dient een berekening te maken van hoe lang de vereiste duur van informatiebeveiliging is “threat timeline”, zie bijlage 2. Dit betreft de bewaartermijn van alle vertrouwelijke gegevens, rekening houdend met “harvest now, decrypt later” (ETSI, 2015).
    - Implementatie van quantum-veilige algoritmes.

Het merendeel van de organisaties die zijn geïnterviewd zijn nog niet zover. Een oorzaak hiervan is dat deze organisaties zich nog niet voldoende bewust zijn van met name de doorlooptijd en impact. Het standpunt vanuit de literatuur dat een quantum computer cryptografie kan doorbreken wordt door alle ondervraagden onderkend.

Investeer in people, proces en technology en start vandaag.

*Beperkingen van het onderzoek*

Ten tijde van dit onderzoek bevonden de ondervraagde organisaties zich in de beginfase van wat vergeleken kan worden met de beginfase van toen traditionele computers in aantocht waren. Hierdoor is de 'kansen' kant in dit onderzoek minder belicht. Ook is in deze scriptie niet uitgebreid ingegaan op hoe beleidsmakers de toepassingsgebieden van quantumtechnologie, zoals quantum computing, quantum sensing en het quantum internet op een maatschappelijk verantwoorde manier kunnen reguleren. Als suggestie voor een vervolgonderzoek kan worden gedacht aan de optimalisatiemogelijkheden die quantumcomputers bieden voor organisaties (use case afhankelijk) maar een interessant perspectief is ook of ethische kwesties een rol moeten spelen in regulering.

*Persoonlijke reflectie*

Mijn persoonlijke interesse in dit onderwerp is groot. In de afgelopen jaren heeft digitalisatie de wereld enorm veranderd. Door de digitale revolutie is digitale communicatie een voorwaarde geworden voor het succes van organisatie.
De impact van quantum computing, zowel qua kansen als bedreigingen zal groot zijn. De invloed van deze technologische ontwikkelingen zullen ook ingrijpend zijn voor de auditprofessie. Daarom is het relevant om te investeren in IT- en datagedreven kennis en vaardigheden.

Mijn persoonlijke leerresultaten zijn dat de beveiligingsmaatstaf voor cryptografische schema's met betrekking tot klassieke aanvallen relatief goed begrepen wordt.
Van veelgebruikte cryptografie zijn de beveiligingsparameters zo gekozen dat een cyberaanval op de cryptografie een prijs heeft die ver boven een bepaalde computationele drempelwaarde ligt. De beveiligingsparameters worden van tijd tot tijd bijgewerkt. Organisaties steunen op deze bewezen beveiligingsmechanismen. Dit terwijl post-quantumcryptografie zich nog moet bewijzen, het is tenslotte nog nieuw en daarmee is niet alleen het risico maar ook de noodzaak om actie te ondernemen evident. Daarom moet ongeacht de exacte tijd van de komst van het quantumcomputertijdperk, nu begonnen worden met het voorbereiden van de informatiebeveiligingssystemen om quantumcomputers te kunnen weerstaan.

# 6 Literatuur


Acampora, G. (2019). Quantum machine intelligence. *Quantum Machine Intelligence*, *1*(1-2), 1-3. https://doi.org/10.1007/s42484-019-00006-5

AIVD. (2015). Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2015, 13 april). Bereid u voor op de komst van de quantumcomputer. https://www.aivd.nl/onderwerpen/ informatiebeveiliging/ documenten/publicaties/2015/04/15/bereid-u-voor-op-de-komst-van-de-quantum-computer

AIVD. (2011). Kwetsbaarheidsanalyse spionage (KWAS) - Integrale ...integraalveilig-ho.nl. (2011). https://integraalveilig-ho.nl

Bloemink, S. (2018, 16 mei). *Door nano-draadjes naar Majorana-deeltjes naar qubits*. De Groene Amsterdammer. https://www.groene.nl/artikel/door-nano-draadjes-naar-majorana-deeltjes-naar-qubits

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188-194. https://doi.org/10.1038/nature23461

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature, 549*(7671), 195-202.

Boixo, S., Isakov, S. V., Smelyanskiy, V. N., Babbush, R., Ding, N., Jiang, Z., ... & Neven, H. (2018). Characterizing quantum supremacy in near-term devices. *Nature Physics*, *14*(6), 595-600. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.754.689&rep=rep1&type=pdf

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. Impact of Quantum Computing on Common Cryptographic Algorithms, 7. https://doi.org/10.6028/nist.ir.8105

Communication TNW. (2020, 25 mei). Researchers build sensor consisting of only 11 atoms. Geraadpleegd van https://www.tudelft.nl/en/2020/tnw/researchers-build-sensor-consisting-of-only-11-atoms

cpl.thalesgroup.com

Dassen, R. (2003). Continuous assurance: Het eeuwige talent? *Maandblad Voor Accountancy en Bedrijfseconomie*, *77*(4), 134-137. https://doi.org/10.5117/mab.77.16289

Dunjko, V., & Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain: A review of recent progress. *Reports on Progress in Physics*, *81*(7), Article 74001.

DNB. (2021). Governance: Toezicht beheersing IT risico's. DNB. https://www.dnb.nl/voor-de-sector/open-boek-toezicht-fasen/lopend-toezicht/prudentieel-toezicht/governance/governance-toezicht-beheersing-it-risico-s/

DNB. (2019–2020). DNB Good Practice Informatiebeveiliging 2019/2020. https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf

ECP. (2019). *Essay Verkenning quantumtechnologie*. https://ecp.nl/publicatie/essay-verkenning-quantumtechnologie

Eimers, P. W. A. (2008). *De betekenis van de Accountant in een Dynamische Wereld*. Vrije Universiteit. https://research.vu.nl/files/3058219/277758.pdf

Elliott, R. K. (2002), Twenty-First Century Assurance, in: Auditing. *A Journal of Practice and Theory*, *21*(1), 139-146.

Elzerman, J. M., Hanson, R., van Beveren, L. H. W., Tarucha, S., Vandersypen, L. M. K., & Kouwenhoven, L. P. (2005). *Semiconductor Few-Electron Quantum Dots as Spin Qubits. Quantum Dots: a Doorway to Nanoscale Physics*, 25–95. https://doi.org/10.1007/11358817_2

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ETSI. (2015). *Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges,* 14, https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

European Commission. (2020, 17 november). *Ethics guidelines for trustworthy AI*. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

European Telecommunications Standards Institute White Paper No. 8. (2015). Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15-31. https://doi.org/10.1177/1094428112452151

Gramling, A., Maletta, A., Schneider, A., & Church, B. (2004). The role of the internal audit function in corporate governance: *A synthesis of the extant internal auditing literature and directions for future research* (pp.194-244). Journal of Accounting Literature.

Grover, L. K. (1996). Een snel kwantummechanisch algoritme voor het doorzoeken van databases. In *Proceedings of the 28th Annual ACM symposium on theory of computing* (pp. 2012-219). ACM.

Havlíček, V., Córcoles, A. D., Temme, K., Harrow, A. W., Kandala, A., Chow, J. M., & Gambetta, J. M. (2019). *Supervised learning with quantum-enhanced feature spaces*. Nature, 567(7747), 209-212.

Hey, T. (1999). *Quantum computing: an introduction*. Computing & Control Engineering Journal, 10(3), 105–112. https://doi.org/10.1049/cce:19990303

https://www.nist.gov

https://www.mccg.nl/

https://www.tudelft.nl/tnw/over-faculteit/afdelingen/quantum-nanoscience

https://intelligence.weforum.org/topics/a1G0X000006OGsDUAW?tab=data

IIA, (2014). De IAF, één van de pijlers van Good Governance. https://www.iia.nl/actualiteit/nieuws/de-iaf-233233n-van-de-pijlers-van-good-governance

ISO/IEC 27001, (2013). ISO. https://www.iso.org/standard/54534.html

Jong, R. de, L. Kool en R. van Est (2019). Zo brengen we AI in de praktijk vanuit Europese waarden. Rathenau Instituut: Den Haag

Kasivajhula, S. (2006). *Quantum computing*: *A survey*. In Proceedings of the 44th annual Southeast regional conference (pp. 249-253). ACM.

Knill, E. (2010). Quantum computing. Nature, 463(7280), 441–443. https://doi.org/10.1038/463441a

KPMG, (2008). *International Survey of Corporate Responsibility Reporting 2008*. www.kpmg.nl https://home.kpmg/xx/en/home/insights/2020/11/the-time-has-come-survey-of-sustainability-reporting.html

KPMG. (2018). *Trust in Artificial Intelligence*. https://home.kpmg/content/dam/kpmg/uk/pdf/2018/06/trust_in_artificial_intelligence.pdf

Kraaijvanger, C. (2018). De quantummechanica: onbegrijpelijk, maar o zo fascinerend. Scientias. https://www.scientias.nl/kwantummechanica-onbegrijpelijk-o-zo-fascinerend/

Klitzing, K. (2004). *25 Years of Quantum Hall Effect (QHE): A Personal View on the Discovery, Physics and Application of this Quantum Effect 1-16.*

Kurzgesagt, (2019). Kurzgesagt – In a Nutshell! Quantum Computers Explained – Limits of Human Technology. YouTube.

Limperg, Jr., Th. (1932). De functie van de Accountant en de Leer van het Gewekte Vertrouwen',Maandblad voor Accountancy en Bedrijfshuishoudkunde, februari

Makarov, V., Jain, N., Witteman, C., Lydersen, L., Wiechers, C., Elser, D., Marquardt, C., Leuchs, G. (2018). Device calibration impacts security of quantum key distribution. Physical Review Letters, 1–5. https://scholar.google.com/citations?user=Cn1TKZcAAAAJ&hl=en#d=gs_md_cita-d&u=%2Fcitations%3Fview_op%3Dview_citation%26hl%3Den%26user%3DCn1TKZcAAAAJ%26citation_for_view%3DCn1TKZcAAAAJ%3AqjMakFHDy7sC%26tzom%3D-60

Merali, Z. (2015). Quantum 'spookiness' passes toughest test yet. Nature, *525*(7567), 14-15. https://doi.org/10.1038/nature.2015.18255

Mosca, M., & Piani, M. (2020). Quantum Threat Timeline. Global Risk Institute. Retrieved from https://globalriskinstitute.org/publications/quantum-threattimeline/

Mosca, M., & Piani, M. (2021). Quantum Threat Timeline Report. GRI januari 2021. https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, 1–39. https://doi.org/10.6028/nist.ir.8309

Muller, F., & Van Heesch, M. P. P. (2020). *Migration to quantum-safe cryptography: About making decisions on when, what and how to migrate to a quantum-safe situation*. TNO. http://resolver.tudelft.nl/uuid:49ee6aa3-3eca-4c84-8908-02abd49674c1

NCSC. (2020). *Quantum security technologies* - NCSC.GOV.UK. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

NIS Directive. (2020). The Directive on security of network and information systems. (2020, 16 december). Shaping Europe's Digital Future - European Commission. https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

NSA. (2015). Cryptography Today. https://web.archive.org/web/20150815072948/https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

PricewaterhouseCoopers (PwC), (2008). Duurzaamheidbarometer. www.pwc.nl

Parms, J. (2015). *Symmetric vs. Asymmetric Encryption - What are differences?* SSL2BUY. https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Parms, J. (2021). *Diffie-Hellman, RSA, DSA, ECC and ECDSA: Asymmetric Key Algorithms*. SSL2BUY. https://www.ssl2buy.com/wiki/diffie-hellman-rsa-dsa-ecc-and-ecdsa-asymmetric-key-algorithms

Perlner, R. and D. Cooper. (2009). *Quantum resistant public key cryptography: a survey*. In Proc. of IDtrust, ACM, pp. 85-93. http://dx.doi.org/10.1145/1527017.1527028.

Praat, J. (2018). Interne beheersing gedefinieerd. Reader BIV Basics. Vrije Universiteit Amsterdam.

Rapport van de Commissie toekomst accountancysector, (2020). Vertrouwen op controle, 114. https://www.accountant.nl/globalassets/accountant.nl/cta--en-mca-rapporten/vertrouwen-op-controle-2020-01-30.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCfg%3d%3d&_t_q=cta%2brapport&_t_tags=language:nl,siteid:3299f554-3e8b-4a32-8d5a-0d2c2f40da3c&_t_ip=82.72.226.229&_t_hit.id=Macaw_EPiCenter_Foundation_Models_Media_PdfFile/_829ed3c4-1b82-4b67-94e9-200a311a8de1&_t_hit.pos=1

Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*. Advances in Cryptology – ASIACRYPT 2017, 241–270. https://doi.org/10.1007/978-3-319-70697-9_9

Schaller, R. R. (1997). *Moore's law: past, present and future*. IEEE Spectrum, 34(6), 52–59. https://doi.org/10.1109/6.591665

Schuld, M., & Petruccione, F. (2018). *Supervised Learning with Quantum Computers.* Springer.

Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. *Contemporary Physics*, *56*(2), 172-185.

Seife, C. (2005). *What Are the Limits of Conventional Computing?* Science, 309(5731), 96. https://doi.org/10.1126/science.309.5731.96

Shannon, C. E. (1948). *A Mathematical Theory of Communication*. Bell System Technical Journal, 27(4), 623–656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, 124-134. IEEE.

Starreveld, R. W., & Leeuwen, V. O. C. (2002). *Bestuurlijke-informatieverzorging 1 Algemene grondslagen* (5de ed.). Noordhoff.

Steane, A. (1998). *Quantum computing. Reports on Progress in Physics*, 61(2), 117–173. https://doi.org/10.1088/0034-4885/61/2/002

Summers, N. (2018, January). *This is what a 50-qubit quantum computer looks like.* Geraadpleegd van https://www.engadget.com/2018-01-09-this-is-what-a-50-qubit-quantum-computer-looks-like.html?

Swayne, M. (2020). *Four Ways Quantum Computing Will Change Artificial Intelligence Forever*. The quantum daily. https://thequantumdaily.com/2020/01/23/four-ways-quantum-computing-will-change-artificial-intelligence-forever/

Tavernier, W., (2001). *De intelligentie van de toekom Geïnterviewde: een praktische en filosofische reflectie over de grenzen en de toekomst van de machine*. lib.ugent.be. https://libstore.ugent.be/fulltxt/RUG01/000/726/934/RUG01-000726934_2010_0001_AC.pdf

TNO. (2019). *Nationale agenda quantum technologie*. Quantum Delta Nederland.

TNO. (2020). *Artificiële intelligentie: Van onderzoek tot toepassing*. https://www.tno.nl/nl/aandachtsgebieden/artificiele-intelligentie/

TU Delft. (2020). News - Quantum Nanoscience. TU Delft. https://www.tudelft.nl/tnw/over-faculteit/afdelingen/quantum-nanoscience/news-quantum-nanoscience/

VU Universiteit. (z.d.). *Overzicht Collecties UB Databases*. https://www.ub.vu.nl/nl/collecties/databases/

van Leeuwen, O., Shahim, A., & Wallage, P. (2015). Inleiding op het thema Digitale Transformatie. *Maandblad Voor Accountancy en Bedrijfseconomie*, 89(11), 402–403. https://doi.org/10.5117/mab.89.31195

Vermaas, P., Nas, D., Vandersypen, L., Elkouss Coronas, D., Asveld, L., Cramer, J., Dobrovitski, S., Evers, W., Munoz, J. F., Janssen, M., Meinsma, A., Steele, G., Taminiau, T., Versluis, R., & Vuik, K. (June, 2019). Quantum Internet: The internet's next big step. TU Delft. https://issuu.com/tudelft-mediasolutions/docs/quantum_magazine_june_2019

Wallage, P., & Van Leeuwen, O. (2017). De interne auditfunctie als onderdeel van de internal governance van een organisatie. *Maandblad Voor Accountancy en Bedrijfseconomie*, *91*(5-6), 137-145. https://doi.org/10.5117/mab.91.24033

Wallucks, A., Marinković, I., Hensen, B., Stockill, R., & Gröblacher, S. (2020). A quantum memory at telecom wavelengths. *Nature Physics*, *16*(7), 772-777.

Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). CJAR, 14(1), 2013, 69-71. Review Essay. DOI: https://doi.org/10.33524/cjar.v14i1.73

Ying, M. (2010). Quantum computation, quantum theory and AI. Artificial Intelligence, 174(2), 162–176. https://doi.org/10.1016/j.artint.2009.11.009

# 7 Bijlage 1

*Tabel 5: Systemen voor digitale beveiliging: Asymmetrische sleutelalgoritmes*

| Beveiligingsteunt algoritme | Jaar | Kraakmechanisme | Vereist geheime sleutel | Vereist openbare sleutel | Beveiligingsmechanisme | Cryptografie wordt doorbroken door Quantumcomputer |
|---|---|---|---|---|---|---|
| Diffie-Hellman-algoritme | 1977 | Vereist delen van een "geheime" sleutel tussen twee communicerende partijen. De sleutels worden gegenereerd door grote priemgetallen te vermenigvuldigen. | √ | | Bij gebruik van authenticatie is Diffie-Hellman echter kwetsbaar voor man-in-the-middle-aanvallen, waarbij de derde partij communicatie kan onderscheppen en zich voordoet als een geldige deelnemer aan de communicatie tijdens het wijzigen of stelen van informatie. Het is rekenkundig gezien moeilijk voor een externe hacker om de privésleutels af te leiden. | √ |
| Rivest Shamir Adleman (RSA) | 1983 | Combineren twee algoritmen te: het een toegepast op asymmetrische cryptografie, of PKI (Public Key Infrastructure), en het andere algoritme zorgt voor veilige digitale handtekeningen. de afzender een hash-waarde van het bericht, die dezelfde encryptiesleutel gebruikt als het ondertekenscenario. De ontvanger doet dezelfde hash-waarde aan de ontvangende kant en op hetzelfde manieren te komen, vaarmee de beveiligde handtekening wordt bevestigd. Het RSA-algoritme heeft drie hoofdprocessen: genereren van sleutelparen, codering en decodering. De sleutels worden gegenereerd door grote priemgetallen te vermenigvuldigen. | √ | √ | De openbare sleutel wordt verzonden via een onbeveiligd kanaal, maar de privésleutel blijft geheim en wordt niet verstrekt aan de openbare sleutel, maar kunnen alleen worden ontsleuteld met de privésleutel. De digitale handtekening van RSA heeft echter een kwetsbaarheid, waardoor brute-force-aanvallen de privésleutel kunnen decoderen, en blootgesteld aan specifieke aanvalstypen zoals zijkanaalanalyse, timingaanvallen en andere. Bovendien is er sprake van computationele overhead bij RSA, en met name in mobiele en tabletomgevingen, waardoor het prestatieproblem groot is. De sleutellengte is ook een punt van zorg, aangezien RSA-sleutels en 2048-bits lang moeten zijn, omdat gezien de vooruitgang in cryptografie en computerbronnen, 1024-bits sleutels onvoldoende veilig worden geacht tegen verschillende aanvallen. | √ |
| Digital Signature Algorithm (DSA) | 1991 | De National Security Agency (NSA)ontwikkelde DSA als alternatief voor het RSA-algoritme. Het National Institute of Standards and Technology (NIST) gaf het algoritme zijn goedkeuring als door de Amerikaanse overheid goedgekeurde en gecertificeerde versleutelingsregeling die dezelfde mate van beveiliging bood als RSA, maar verschillende wiskundige algoritmen gebruikt voor ondertekening en versleuteling. Net als RSA is DSA een asymmetrisch versleutelingsschema, of PKI, dat een paar sleutels genereert, een openbare en een privé. | √ | √ | De handtekening wordt privé gemaakt, hoewel deze openbaar kan worden geïdentificeerd; het voordeel hiervan is dat slechts één autoriteit de handtekening kan aanmaken, maar elke andere partij kan de handtekening valideren met de publieke sleutel. DSA is daardoor sneller bij het ondertekenen, maar langzamer bij het verifiëren; Daarom is DSA een verstandige keuze als er meer prestatieproblemen aan de clientzijde zijn. DSA en RSA kunnen samen worden uitgevoerd onder sommige serversystemen. Omdat DSA en RSA echter zo op elkaar lijken, zijn ze onderhevig aan vergelijkbare aanvallen, en RSA is overgestapt op langere sleutels, wat DSA nog niet heeft gedaan. | √ |
| Elliptic Curve Cryptography (ECC) Elliptic Curve Digital Signature Algorithm (ECDSA) / Suite B | 1985/2005 | Cryptografische algoritme dat is ontwikkeld voor verhoogde beveiliging en robuustere netwerkprotocollen. Sommige onderzoekers hebben bewezen dat ECC-cryptografie net zoveel sterke beveiliging kan bieden met een 164-bits sleutel als andere systemen berekend met een 1024-bits. ECC-cryptografie helpt om een beveiligingsniveau tot stand te brengen dat gelijk is aan of groter is dan RSA of DSA, de twee meest algemeen aanvaarde versleutelingsmethoden - en het doet dit met minder computationele overhead, verwat minder verwerkingskracht en gaat veel verder dan de mobiele ether bij de implementatie. | √ | √ | ECDSA (Elliptic Curve Digital Signature Algorithm) is gebaseerd op DSA, maar gebruikt nog een andere wiskundige benadering voor het genereren van sleutels. ECC is een op zichzelf staande wiskundige vergelijking, maar ECDSA is het algoritme dat op ECC wordt toegepast om het geschikt te maken voor beveiligingsencryptie. Net als RSA en DSA, is het een ander asymmetrisch cryptografisch schema, maar in ECC definieert de vergelijking het publieke - private sleutelpaar door bewerkingen op punten van elliptische krommen, in plaats van het te berekenen als het product van twee grote priemgetallen. | √ |

# 8 Bijlage 2

**Threat Timeline**

De urgentie voor een specifieke organisatie om de overgang naar quantum-veilige cryptografie voor een bepaald cybersysteem vertrouwt op drie eenvoudige parameters[7]:

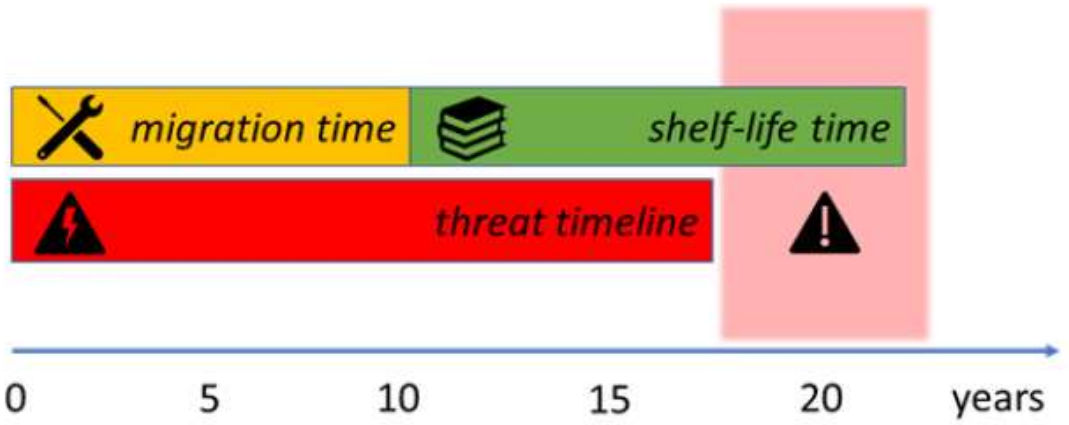
*x = "hoeveel jaar moet informatie veilig blijven" (shelf-life time)*

*y = "hoeveel jaar heeft de organisatie nodig om haar IT-infrastructuur quantum-veilig te maken" (migration time)*

*z = "hoeveel jaar duurt het voordat een grootschalige quantum computer evident is" (threat timeline)*

Als $(x + y) > z$, moeten organisaties dringend maatregelen nemen, omdat organisaties niet in staat zijn om hun assets te beschermen voor de vereiste jaren (shelf-life time).

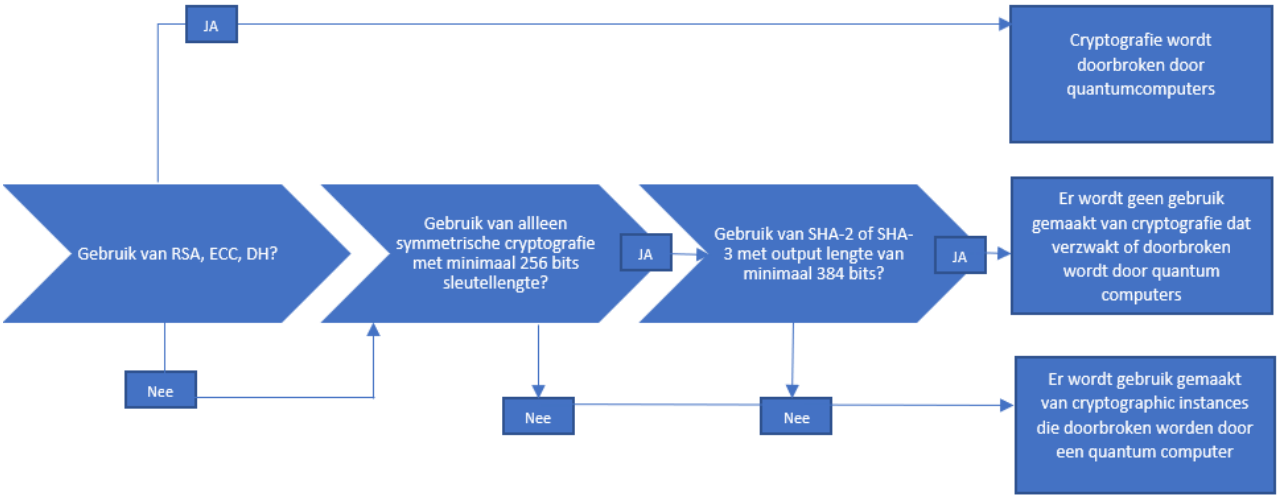
Als een grootschalige quantum computer ($z$) gebouwd is voordat de infrastructuur quantum-veilig is en de vereiste duur van informatiebeveiliging is verstreken ($x + y$), dan is de versleutelde informatie niet veilig en dus kwetsbaar voor aanvallen.




*Figuur 7: Herdrukt van ''Quantum Threat Timeline Report 2020'' door Mosca, M. & Piani, M. (2020), p.7. Global Risk Institute.*

# 9 Bijlage 3

Organisaties kunnen als quick scan de onderstaande flowchart gebruiken om te bepalen of ze gebruik maken van kwetsbare cryptografie.




*Figuur 8: Quick scan gebruik van kwetsbare cryptografie (Muller, F., & Van Heesch, 2020)*

## 10 Bijlage 4

De getranscribeerde interviews en coderingschema zijn vanwege de omvang niet als bijlage opgenomen. De interviews en het coderingschema in Excel kunnen indien gewenst los worden opgevraagd door de Vrije Universiteit. Dit is alleen bestemd voor interne validatie door ITACA Vrije Universiteit Amsterdam en mag niet verder worden verspreid.