Autor: Bundesquantenallianz, 02.01.2025

www.bundesquantenallianz.de

Positionspapier zur Vorbereitung der Bundesorganisationen und Behörden auf den Q-Day

Aktuelle Situation

Die Entwicklung von Quantencomputern hat in den vergangenen vier Jahren rasant Fahrt aufgenommen, im Jahr 2020 wurden Quantencomputer mit ca. 20 Qubits vorgestellt, 2024 werden bereits mehr als 1.000 Qubits zur Verfügung gestellt. Die weitere Entwicklung und Skalierung dieser Technologie ist momentan nur schwer exakt vorherzusagen. Klar ist nur, dass die Verfügbarkeit von ausreichend performanten Quantencomputern ein existentielles Risiko für die bestehenden und jetzt im Einsatz befindlichen kryptographischen Algorithmen und Systeme darstellen.

Das Global Risk Institute hat hierzu in seiner "Quantum Threat Timeline 2023" 37 international führende Experten aus Forschung und Industrie befragt. Von diesen schätzen 17 das Risiko der Verfügbarkeit von kryptographisch relevanten Quantencomputern innerhalb der nächsten zehn Jahre höher als 5% ein. Darüber hinaus sagen 10 der Befragten sogar, dass sie eine Eintrittswahrscheinlichkeit von 50% oder höher für dieses Ereignis sehen.

Insofern muss die Beschäftigung mit Quantencomputing und den damit einhergehenden Chancen und Risiken für die digitale Infrastruktur als wesentlich und relevant angesehen werden. Insbesondere betrifft das die Beschäftigung mit möglichen Quantenrisiken im Kontext des Cybersecurity Risikomanagements.

Neben der technologischen Entwicklung und den damit einhergehenden Auswirkungen für die Sicherheit digitaler Systeme ist unbedingt aber auch die industriepolitische Bedeutung zu beachten. Der Draghi Report vom August 2024 benennt hierbei im Wesentlichen zwei Dimensionen: Neben den bereits beschriebenen Auswirkungen auf die Sicherheit der existierenden digitalen Infrastrukturen benennt er Quantencomputing als einen der wesentlichen neuen Bausteine der digitalen Ökosysteme der nächsten Generation, die in den nächsten 15-Jahren im dreistelligen EURO Milliardenbereich zum EU Binnenmarkt beitragen könnten.

Die teilweise schon stattfindende Quanten-„Revolution" hat dabei mehrere Dimensionen, mindestens vier sind hier zu nennen:

1. Die bestehende in breiter Fläche verbaute **Kryptographie** verliert im Moment der Verfügbarkeit von leistungsfähigen Quantencomputern ihre Sicherheit und muss daher ersetzt werden (Stichwort: Kryptoagilität, Krypto Kataster, PQC, QKD).

2. Die **Quanteninformatik** wird die bestehende Informatik revolutionieren und benötigt ganz neuartige algorithmische Denkansätze (**Think Quantum**). Dies erfordert eine breite Vorbereitung auf allen Ebenen, beginnend von der Forschung über die akademische Lehre bis hin zur „praktischen" Umsetzung im öffentlichen und privaten Sektor.

3. Nicht nur ein Wissensaufbau, sondern auch ein **Infrastrukturaufbau** muss auf europäischer und nationaler Ebene vorangetrieben werden, sonst verpasst Europa dieses Zukunftsthema. Hierbei sind auf europäischer Ebene insbesondere die Themen

- „long-term **EU Quantum Chips plans**“ (Mission Letter für Henna Virkunnen, Executive Vice-President designate for Tech Sovereignty, Security and Democracy) sowie
- die „industrial dimensions of Artificial Intelligence, **quantum and high-performance computing**“ im Kontext von innovation and research (Mission Letter für Stephane Sejourne, Vice-President designate for Prosperity and Industrial Strategy)

zu berücksichtigen.

4. Auch bei „kurzfristiger“ Verfügbarkeit von relevanten Quantencomputing Ressourcen ist davon auszugehen, dass **hybride Szenarien** bestimmend sein werden (also ein zweischrittiges Vorgehen, Vorberechnungen auf klassischen Hochleistungsrechnern mit Reduktion des Problems auf ein „quantengeeignetes“, Fortführung der Rechnung auf einer Quantencomputing Infrastruktur (inklusive eventueller klassischer Nachbearbeitung).

Szenarien im Kontext kryptoanalytischer Angriffe

Die Aufzeichnung von verschlüsselten vertraulichen/ geheimen Daten erfolgt bereits heute. Sie können entschlüsselt werden, sobald leistungsfähige Quantencomputer zur Verfügung stehen. Dieses Szenario lässt sich (vorwärtsgewandt) nur durch eine schnellstmögliche Migration der jetzt eingesetzten Verschlüsselungsmechanismen heilen. Bisherige verschlüsselte und durch Dritte aufgezeichnete Kommunikation (data in transit) lässt sich durch die ursprünglichen Sender der Information naturgemäß nicht mehr „umschlüsseln“. Gespeicherte verschlüsselte Nutz-Daten (data at rest) können mit neuen PQC-Mechanismen neu verschlüsselt bzw. um-verschlüsselt werden.

Grundsätzlich ist festzustellen, dass zum heutigen Zeitpunkt noch nicht bekannt ist, dass entsprechend leistungsfähige Quantencomputer bereits jetzt zur Verfügung stehen oder dass dies kurzfristig erfolgen wird. Staaten wie China, Russland arbeiten nachweislich an der Entwicklung von Quantencomputern und das unter massiver Anhäufung und Bündelung von Ressourcen (Milliarden statt Millionen). Diese Quantencomputer könnten von den Staaten für Cyberattacken genutzt werden. Aber auch nationale Plattformen aus anderen Regionen wie USA, Kanada, Japan, UK sind im Aufbau und stehen in Konkurrenz zu europäischen Entwicklungen in Finnland, Frankreich oder Deutschland. Für diese genannten Plattformen ist zu bemerken, dass ein Einsatz dieser Ressourcen für krypt-analytische Zwecke nicht grundsätzlich auszuschließen ist (und in einigen Fällen sehr wohl davon auszugehen ist, dass diese Ressourcen explizit für diesen Zweck aufgebaut werden). Eine aufzubauende multinationale/länderübergreifende Governance, in der eine entsprechende Plattform betrieben und zur Verfügung gestellt wird, kann helfen, die Anwendung in kryptanalytischen Szenarien zu erschweren. Ausgeschlossen werden kann das aber sicherlich nicht. Insofern kann den kryptanalytischen Bedrohungsszenarien nur durch eine konsequente Umsetzung von Kryptoagilität und PQC begegnet werden.

Szenarien im Kontext des Quantencomputing

Neben den kryptanalytischen Szenarien sind natürlich auch die **konstruktiven** Aspekte und Chancen des Quantencomputings zu betrachten.

Die grundsätzlichen Bemerkungen zu den unterschiedlichen internationalen Ansätzen zum Aufbau von Quantencomputing Plattformen sind auch hier anwendbar: Aktivitäten hierzu erfolgen in nahezu allen großen Regionen der Welt und werden vor allem durch große Plattformanbieter dominiert (bspw. IBM, Alphabet, Nvidia, AWS, Honeywell, Microsoft). Die Frage nach der jeweiligen Governance und der damit verbundenen Verfügbarkeit dieser Ressourcen und Plattformen spielt hierbei eine entscheidende Rolle.

Auch auf europäischer Ebene sind verschiedene Aktivitäten sichtbar, in Finnland baut IQM einen Quantencomputer, in Frankreich arbeitet Pasqal an dem Bau eines Quantencomputers.

In Deutschland werden zahlreiche Aktivitäten im Quantencomputing auf Landes- und Bundesebene durchgeführt und können durchaus vorzeigbare Ergebnisse vorweisen. Allerdings ist festzustellen, dass die nationalen Entwicklungen nicht mit den internationalen Aktivitäten schritthaten können.

Es ist daher notwendig, den u.a. mit der DLR Quantencomputing Initiative (QCI) begonnenen Weg zur Entwicklung von Quantensystemen zu fokussieren und zu intensivieren und auf die zum heutigen Wissensstand erfolgversprechendsten Technologien zu konzentrieren, dies betrifft die Hardwareentwicklung ebenso wie die Softwareentwicklung.
Ein föderaler Ansatz mit Quantenzentren in jedem Bundesland hält nicht Schritt mit der internationalen Entwicklung. Es gilt vielmehr in einem zentralen Ansatz das vorhandene große Potential im Umfeld Quanten-Software-Architektur, Quantenalgorithmen und Benchmarking zu heben, um Quantencomputing erfolgreich zu machen.

Wie bereits oben ausgeführt sind große Plattformen vornehmlich nordamerikanischer Provenienz als führend im Aufbau von großen und skalierbaren Quantencomputing Ressourcen anzusehen. Es entstehen dadurch kommerzielle, industriepolitische und geopolitische Abhängigkeiten analog etwa zur bestehenden Cloudsituation. Daraus ergeben sich sowohl Fragen datenschutzrechtlicher Art (Abfluss von Daten aus dem Gültigkeitsbereich der DSGVO) aber auch industriepolitischer und insbesondere sicherheitspolitischer Art (Governance der kommerziellen Verfügbarkeit von Ressourcen für Dritte, die eventuell Cyberattacken auf Basis von Quantencomputing durchführen wollen).

Zusammenfassend lässt sich also festhalten:
Die Bedeutung technologischer Souveränität auf dem Feld des Quantencomputing ist als wesentliche Voraussetzung dafür anzusehen, die enormen Potentiale dieser neuen Technologie (siehe die Aussagen des Draghi Reports) für Deutschland und Europa zu heben. Hierfür, also zur Schaffung und Sicherstellung von technologischer und digitaler Souveränität für Deutschland und Europa sind jetzt die mutigen Entscheidungen zu Technologien und den damit verbundenen Investments zu treffen. Nur auf dieser Basis besteht die Chance, die benannten Abhängigkeiten im Hinblick auf technologische und digitale Souveränität, Datenschutz und sicherheitspolitischer Relevanz auf nationaler und europäischer Ebene zu minimieren und im Driver Seat zu bleiben.

Empfehlungen der Bundesquantenallianz

Zentrale Informationsquelle schaffen

Der Fortschritt der Entwicklung von Quantencomputern und die möglichen kryptographischen Gegenmaßnahmen sind für viele IT-Experten und für einen Großteil der Entscheider Neuland und daher schwierig zu bewerten. Es sind bereits Unternehmen in der Bundesrepublik tätig, um teils fehlerbehaftete Informationen zu ihrem Zwecke zu nutzen und Umsatz zu generieren – mit fragwürdigem Mehrwert für den Auftraggeber. Die Nachricht des vermeintlichen Durchbruchs von Alphabet im November 2024 hat die Medien geflutet, obwohl der Fortschritt bei genauerer Analyse eher überschaubar ist.
Allerdings ist aufgrund der umfangreichen weltweiten Investments mit einem Durchbruch in absehbarer Zeit zu rechnen und eine Einschätzung sollte den Experten vorbehalten sein. Daher empfehlen wir in Anlehnung an die 2022 gegründete Bundesquantenallianz die Schaffung eines neutralen Think Tanks für Behörden und Bundesunternehmen zum Informationsaustausch, Aus- und Weiterbildung von Mitarbeitern sowie zur Beratung von Bundeseinrichtungen und politischen Gremien. **Es braucht eine souveräne, herstellerunabhängige und die gesamte Quantentechnologie umspannende Einrichtung, die es dem Bund erlaubt, souverän und technologisch führend die Quantentechnologien zu bündeln.**
Der Bund muss innerhalb der Ressorts und auch ressortübergreifend Quantentechnologien verstehen, nutzen und beherrschen.

Wir benötigen eine pro-aktive und moderierende Rolle auf Bundesebene, um die Landes- und Einzel-Bundesressortebene zu orchestrieren (vgl. diverse Initiativen auf Landes Ebene wie Munich Quantum Valley, Lower Saxony Quantum Valley, EIN Quantum NRW, die Programme im BMBF, BMWK und BMF).

Dies betrifft zum einen die Kryptographie als eine zentrale Komponente zur Wahrung der nationalen Sicherheit. Die geopolitischen Auswirkungen der Quantentechnologie werden immens sein – politisch, wirtschaftlich und gesellschaftlich.
Dies betrifft aber auch die konkreten Anwendungspotentiale, die sich aus der Nutzung von Quantencomputern für Use-Cases aus der Bundes- und Landesverwaltung durch Anwendung quanten- und quanteninspirierter Mechanismen und Algorithmen bereits jetzt ergeben können.
Ein weiteres Feld, in dem die Kompetenz des Bundes dringend ausgebaut werden muss, ist das der Quantenkommunikation. In dieser Technologie werden entweder über Quanteneffekte Kommunikationsnetzwerke abgesichert oder durch direkte Kommunikation von Quantum Entitäten (Direct Secure Quantum Communication) wird die Effizienz und Skalierung überhaupt erst ermöglicht.

Pro-aktiven Algorithmenaustausch ermöglichen (Krypto-Agilität)

Im Dezember 2022 wurde vom Weißen Haus der Quantum Preparedness Act verabschiedet, um die US-Bundesbehörden auf den Q-Day vorzubereiten. Es mussten innerhalb weniger Monate Masterpläne zur Einführung von Krypto-Agilität erstellt werden, obwohl die einzusetzenden quantensicheren Algorithmen noch nicht final verabschiedet waren. Die EU hat im April 2024 eine Empfehlung zur Einführung von Krypto-Agilität gegeben, eine Arbeitsgruppe aus Vertretern von 20 europäischen Ländern sind einer ersten Sitzung zusammengekommen. Sie haben sich zum Ziel gesetzt, innerhalb von 2 Jahren ein Vorgehen für die europäischen Staaten zu erarbeiten. Die Gruppe setzt sich aus europäischen Bundesbehörden zusammen.
Aufgrund der strategischen Verankerung von Quantencomputing in USA und China und dem damit verbundenen rasanten Fortschritt im Quantencomputing empfehlen wir den Zeitplan deutlich zu straffen und neben den Bundesbehörden auch Bundesunternehmen an den Vorbereitungen zu beteiligen, um die Operationalisierung der Vorgaben sicherzustellen.
Die Bundesquantenallianz bietet hierzu ihre umgehende Mitarbeit an.

Toolstack aus europäischen Tools aufbauen und Behörden sowie Industrie zur Verfügung stellen

Zur Einführung von Krypto-Agilität sind verschiedene Tools für Scan, Aufbau des Inventory, Testbed, Priorisierung, CI/CD Pipeline erforderlich.
Die Hersteller, in den meisten Fällen große US-Unternehmen, die auch Cloud-Services anbieten, betten diese Tools sukzessive in ihre Value-Chain ein. Da es sich um unternehmenskritische Daten handelt und ein Vendor-Lockin unbedingt vermieden werden sollte, gilt es die Produkte europäischer Hersteller zu prüfen und ggf. einzusetzen.
Wir empfehlen daher, einen Toolstack aus europäischen Tools aufzubauen und die vielleicht vorhandenen Whitespots durch europäisch besetzte Projekte zu schließen.

Quantum Thinking aufbauen und stärken

Um die Investitionen in die Technologie auch für zukünftige Legislaturperioden sicherzustellen, muss die konstruktive Seite des Quantencomputings stärker präsent gemacht werden.

Hierzu ist erforderlich:
- Starker Fokus von Lehre und Forschung auf Quantencomputing und Quantenalgorithmik (Quanteninformatik) mit finanzieller Ausstattung der Einrichtungen

- Fokus auf hybride Szenarien HPC/QC und industrielle Anwendungsfälle zum Nachweis der Quantum Advantage
- Verstärkte Betrachtung von quantum inspired Algorithmen
- Verbindungen zwischen verschiedenen Quantentechnologien aufzeigen (z.B. „Verschränkung“ von QKD und Quantum Computing, siehe Berlin Falling Walls Background Table 2024)

Quantum Souveränität für Deutschland und Europa schaffen

Durch eine entsprechende Governance kann der missbräuchliche Einsatz durch Dritte etwa im Kontext von Cyberattacken verhindert oder zumindest deutlich erschwert werden. Deutschland kann und muss bei der Konzeption und dem Aufbau dieser Infrastruktur eine wesentliche Rolle spielen.