# Steckbrief Quantencomputing

Perspektiven für den Verteidigungssektor | Juli 2020

**AK Verteidigung:** PG IT-Innovationen **Thema:** Quantencomputing

## Ausgangssituation

**Beschreibung:**

- Unter Quantencomputing (QC) versteht man die Nutzung von Effekten auf Quantenebene zur Berechnung von Daten
- Je nach Implementierung ist diese oftmals nur bei Extremtemperaturen nahe absolutem Nullpunkt (-273,15°C) durchführbar
- Bereits jetzt ist eine Brückentechnologie auf Silikonchipbasis unter Normalbedingungen für bestimmte Anwendungen verfügbar
- Aktuelle Quantencomputer haben nur circa 50 Quantenbits (Qubits) – für sinnvolle Anwendungen sind mindestens mehrere hundert notwendig
- In bestimmten Anwendungsfällen könnten Quantencomputer klassischen Computern deutlich überlegen sein
- Quantencomputer können z.B. echte Zufallszahlen erzeugen, was für viele Algorithmen ein Vorteil ist
- Quantencomputer können die mathematischen Probleme, auf denen asymmetrische Kryptografie beruht deutlich schneller berechnen als klassische Computer. Quantencomputer können so gängige asymmetrische Kryptografieverfahren brechen, deren Sicherheit auf der Laufzeit für Faktorisierungsverfahren beruht sowie die Sicherheit von symmetrischer Kryptographie halbieren
- Quantenschlüsselverteilung wird vermutlich den Austausch von symmetrischen Schlüsseln für sichere Kommunikation erlauben

**Bewertung:**

- Vorteilen von Quantencomputern stehen gegenwärtig noch viele Probleme bei der technischen Realisierung gegenüber; Entwicklung ist aber nicht Frage des »Ob?«, sondern des »Wann?«
- QC wird klassische Arbeitsplatzrechner oder Rechenzentren nicht ersetzen
- Brückentechnologien auf Basis des »Quanten-inspired Computing« sind schon heute mit QC-Algorithmen nutzbar. Diese sind in der Lage Lösungen für signifikante Problemgrößen zu liefern und fügen sich nahtlos in bestehende Datacenter Infrastruktur ein
- Auch hybride Systeme sind denkbar, welche die Vorteile beider Systeme in sich vereinen
- Das Brechen heute gängiger Verschlüsselungen durch QC stellt ein Sicherheitsrisiko für Streitkräfte dar.

## Gemeinsames Ziel/Nutzungspotentiale

- Nutzung in der Geoinformatik
- Verbesserung der Aufklärung > Fähigkeit aus komplexen Datenmengen Lagebilder zu erstellen
- Revolution von Kryptierverfahren, Kryptoanalyse, Resilienzverbesserung > Post Quanten-Kryptographie
- Optimierungen in der Logistik (Routen- und Lageroptimierung) sowie finanzmathematische Berechnungen
- Optimierung der Führungsfähigkeit
- Einsatz als Mittel für die Abwehr ballistischer Raketen
- Neuerungen in der KI und Algorithmensystematik
- Kryptographie, QC-resistente Schlüsseleinigung
- Energieeinsparung, Einsatz in der Materialforschung und zum Erkennen des Abstrahlverhaltens / der Reflexionsoptimierung

bitkom

- Cyber Warfare
- Simulation
- Operations Research
- Schließen von Fähigkeitslücken z.B. im Bereich quantenresistenter Verschlüsselung
- Cyberdefense, z.B. durch Erkennung von Anomalien
- Big Data Analysis und Deep Learning

## Stellgröße

- Schnelligkeit hinsichtlich F&E zur Nutzung in realen Umgebungen
- Effizienz (Verringerung des Ressourceneinsatzes zur Erlangung einer bestimmten Wirkung)
- Effektivität (Verbesserung des Wirkungsgrades bestimmter Funktionalitäten)
- Optimierungen in Bereichen klassischer Verfahren (Digital Annealing / Quantum Annealing = Abweichung von Optimum vs. Rechenzeit)
- Erkennen und Bewerten von Bedrohungsszenarien inkl. der Fähigkeit zur Reaktion
- Erreichen von Benchmark-Werten im internationalen Bereich (Outcome-orientiert)
- Verfügbarkeit und Zugang zu QC als Stellgröße
- Neue Anwendungsfelder erschließen, z.B. Optimierungen, die mit klassischen Ansätzen schwierig sind
- Quantencomputerresistente Verfahren (Post-Quanten-Kryptographie, Schlüsseleinigung, Protokolle) entwickeln
- Fehlerkorrekturverfahren von QC verbessern, um Rauschen der Qubits zu kompensieren
- Qualität / Wirkungsgrad von Algorithmen

## Maßnahmen/Vorgehensweise

- Entwicklung einer grundlegenden Idee für den Verteidigungssektor, wozu QC eingesetzt und genutzt werden kann, wie dies bereits in anderen Sektoren erfolgt ist
- Abschätzung, mit welcher Geschwindigkeit sich die Fähigkeiten von Quantencomputer nin den nächsten Jahren entwickeln wird und wo diese ihre Anwendung finden
- Vorbereitung auf eventuellen Technologiesprung, sowohl bei der Hardware als auch bei den Algorithmen inklusive der Nutzung vorhandener Brückentechnologien (Nutzung und ggf. Abwehr)
- Der Übergang vom klassischen Computing sollte frühzeitig sichergestellt werden inkl. der Validität klassischer Sicherheitstechnologie (Krypto & Blockchain)
- Der Wettbewerbsnachteil in der Hardwareentwicklung sollte durch gezielte Förderung auf der Anwendungsseite ausgeglichen werden
- Quantencomputing kann für viele Anwendungsbereiche »Quantensprünge« generieren, noch aber ist der Schwerpunkt (Ressourceneinsatz) eindeutig auf den Bereich der Forschung zu legen
- Brückentechnologien nutzen die gleichen Algorithmen wie QC und bieten schon jetzt die Möglichkeit des Know-how Aufbaus und Berechnungen für erste Bereiche, z.B. Optimierungen (identisches Ecosystem)
- Krypto-Agilität muss bereits jetzt zum Design-Kriterium erhoben werden
- Die Politik sollte die Verfügbarkeit und den Zugang zu Quantencomputern sicher stellen
- Evaluierung von Ideen zu den Begleittechnologien
- Intensivierung von Forschungsaktivitäten: Welche Anwendungen lassen sich sinnvollerweise mit QCs rechnen, ggf. auch schon mit wenigen Qubits als Optimierungen, die mit klassischen Ansätzen schwierig wären