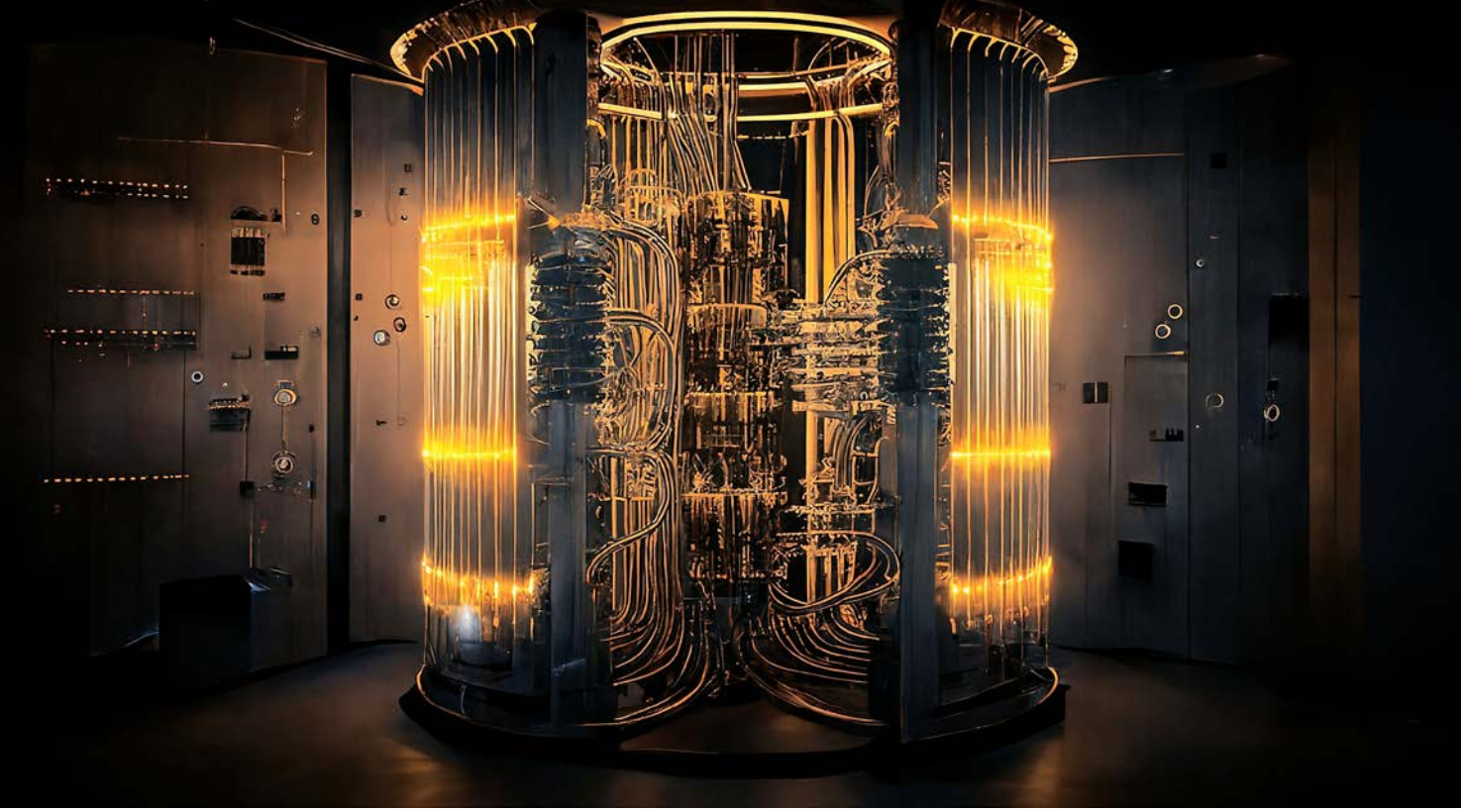

Foto: Sean Song - stock.adobe.com

Bisher galten Quantencomputer als Zukunftstechnologie – wenn nicht gar als Science-Fiction. Tatsächlich aber stehen Quantencomputer kurz davor, zumindest in der Forschung „Mainstream“ zu werden.

Quantenwelt der Sicherheit

Wie Cybersecurity im Quantencomputer-Zeitalter aussieht und welche Rolle sie für Kritische Infrastrukturen spielt.

OLIVER WEIMANN & PROF. MARCIN PAWŁOWSKI

Aktuell werden Milliarden-Investitionen in die brennenden Zukunftsthemen KI und Cybersecurity getätigt, in Heilbronn entsteht etwa ein eigenes Zentrum für Künstliche Intelligenz. In genau diesem Zusammenhang nimmt auch das Thema Quantencomputing eine tragende Rolle ein. Bisher gelten Quantencomputer als Zukunftstechnologie – wenn nicht gar als Science-Fiction. Tatsächlich aber stehen Quantencomputer kurz davor, zumindest in der Forschung „Mainstream“ zu werden.

Das finnische Startup IQM hat beispielsweise als erster Anbieter bekannt gegeben, weltweit einen supraleitenden Quantencomputer für Universitäten und Labore anzubieten, welcher weniger als eine Million Euro kostet. Und IBM entwickelt Geschäftsmodelle für Quantencomputing-as-a-Service. Damit werden wichtige Meilensteine erreicht, mit denen gleichzeitig riesige Erwartungen einhergehen.

Quantencomputing verbindet die Quantenphysik mit der Informatik und verspricht bislang nicht für möglich gehaltene verfügbare Rechenleistung. Damit birgt die Quanteninformatik erhebliches Potenzial im Rahmen der Lösung komplexer Herausforderungen: So werden signifikant präzisere Wettermodelle oder „Quantensprünge“ in der Medikamenten- und Materialforschung prognostiziert. Gemeinsam mit der voranschreitenden KI stehen wir also vor einem technologischen Wendepunkt.

„Kritische Infrastrukturen, Verbindungsknoten, autarke Netze und Satellitenkommunikation können durch Quantenkryptographie geschützt werden.“

Oliver Weimann, Co-Founder & CEO der Quantum Cybersecurity Group.

Cyber-Risiken durch Quantencomputer

Bei all den Möglichkeiten und Vorteilen, die die Entwicklung von Quantencomputern mit sich bringt, müssen allerdings auch die Risiken betrachtet werden. Aufgrund ihrer bislang unvorstellbaren Rechenleistung sind Quantencomputer in der Lage, heutige Standardverschlüsselung, also asynchrone Schlüssel, innerhalb von wenigen Minuten, teilweise innerhalb von Sekunden, zu brechen. Damit wird die gesamte Cybersecurity auf den Kopf gestellt und die bisherige „Standardsicherheit“ kann in der Form nicht mehr gewährleistet werden.

Das bedeutet, der Zugang zu Bankkonten, persönlichen Krankenakten, Geheimrezepturen oder geheimen Firmeninformationen ist zukünftig nicht mehr geschützt. Gerade vor dem Hintergrund

exponentiell gestiegener politischer Spionage und kommerziell motivierter Cyberangriffe ist das Risiko erfolgreicher Cyber-Angriffe also greifbar.

Besonders die Bereiche der Kritischen Infrastruktur (Kritis) sind von dem erhöhten Risiko betroffen. Kritische Infrastrukturen stellen Strom und Wasser zur Verfügung, sichern die Mobilität und die medizinische Versorgung. Sie umfassen all die Einrichtungen und Systeme, die ein Gemeinwesen braucht, um zu funktionieren. Fallen sie aus, kann das zu erheblichen Problemen bei der Versorgung und im Kontext der öffentlichen Sicherheit führen.

Weltweit sind Kritische Infrastrukturen immer stärker durch Cyber-Angriffe bedroht. Wie der Digitalverband Bitkom kürzlich bekanntgab, entstehen der deutschen Wirtschaft durch Diebstahl von IT-Ausrüstung und Daten, durch digitale und analoge Industriespionage und Sabotage pro Jahr mehr als 200 Milliarden Euro Schaden. Ohne geeignete Mechanismen zum Schutz Kritischer Infrastrukturen gibt es zwei Hauptstrategien für Cyberangriffe in diesen Bereichen.

Zum einen zielen Cyberangriffe häufig auf die Störung des Betriebs sowie von Aufsichts- und Wartungsprozessen ab. So können durch Manipulation der Störungs- und Qualitätsmessgeräte unnötige Wartungen oder Notfälle ausgelöst werden oder durch die Übernahme der Kontrolle über diese Geräte Fernabschaltungen von beispielsweise Stromnetzen, Verkehrsampeln, Notfallsystemen auf Bohrinseln oder Kühlsystemen in Kernkraftwerken ausgelöst werden.

Besonders kritisch wird es, wenn ganze Systemgruppen übernommen werden und somit die installierte Hardware bewusst beschädigt und zerstört wird. Hierbei geht es nicht mehr um temporäre Ausfälle, sondern massive langfristige Beeinträchtigungen und erhebliche finanzielle Verluste.

Was Quantum-Cybersecurity bedeutet und wie sie bei der Absicherung helfen kann

Glücklicherweise kann die Quantenphysik helfen und hält neue Lösungen für die Cybersicherheit bereit. Mit Hilfe von Quantentechnologie ist es zum Beispiel erstmals möglich, mathematisch nachweisbar, nicht zu knackende Verschlüsselungstechnologien zu entwickeln – sowohl für heutige Standardcomputer als auch für „zukünftige“ Quantencomputer. Hierbei muss zwischen Quantenkryptographie und Post-Quanten-Kryptographie unterschieden werden:

Die Quantenkryptographie nutzt quantenmechanische Effekte, um eine sichere Übertragung der verwendeten Schlüssel zu gewährleisten. Im Gegensatz zu bisherigen kryptographischen Verfahren bilden also physikalische Effekte und nicht mathematische Annahmen (Algorithmen) die Grundlage, sodass die synchrone Verschlüsselung gewählt werden kann. Dies führt gleichzeitig zur Erfordernis physischer Komponenten beim Aufbau einer quantenkryptischen Lösung.

„Aufgrund ihrer bislang unvorstellbaren Rechenleistung sind Quantencomputer in der Lage, heutige Standardverschlüsselung, also asynchrone Schlüssel, innerhalb von wenigen Minuten, teilweise innerhalb von Sekunden, zu brechen.“

Prof. Marcin Pawłowski, Head of Centre for Theory of Quantum Technologies an der Universität Danzig sowie Co-Founder der Quantum Cybersecurity Group.

Quantenverschlüsselung auf Basis von Quantum-Key-Distribution (QKD) nutzt miteinander „verstrickte“ Photonen, um die sichere Übertragung von synchronen Schlüsseln zwischen Sender und Empfänger zu realisieren. Das bedeutet technisch gesehen, dass zwei Photonen an unterschiedlichen Orten zu demselben Zeitpunkt Informationen bereitstellen können, welche eineindeutig als Teil einer Verschlüsselung verwendet werden können. Der positive Nebeneffekt liegt darin begründet, dass in der Quantenphysik die Beobachtung ein Eingriff in das System bedeutet und das Ergebnis verändert. Somit ist ein Abfangen des Schlüssels auf dem Übertragungsweg schlichtweg nicht möglich.

Von Natur aus nicht deterministisch

QKD-Protokolle verwenden Zufallszahlen, deren Sicherheit von der Qualität der verwendeten Zufallszahlengeneratoren abhängt. Auch hier nutzt man Quantenphysik, da die Verteilung von Lichtpartikeln weder vorhersehbar noch beeinflussbar ist. Sogenannte Quantum Random Number Generators (QRNGs) erzeugen Zufälligkeit, die von Natur aus nicht deterministisch ist. Die Vorteile liegen etwa in der Nutzung von Quantenunbestimmtheit und in der Fähigkeit, den Ursprung der Unvorhersehbarkeit zu verstehen und zu verifizieren – was eine wichtige Voraussetzung für die gesamte Cybersicherheitskette ist.

Die Post-Quantum-Kryptografie hingegen beruht auf mathematischen Methoden, um die Kryptografie von heute auch ohne den Einsatz von Quantentechnologie auf das Quantencomputing vorzubereiten. Hierfür wurden zahlreiche verschiedene Verfahren und Algorithmen entwickelt, die vom NIST (National Institute of Standards and Technology) getestet und standardisiert wurden. Beide Methoden der quantensicheren Kryptografie sind für unterschiedliche Anwendungsfälle geeignet. In Zukunft sehen wir tendenziell eine Kombination aus beiden Verfahren auf Basis sicherer Quantenschlüssel.

Lokale Kritische Infrastrukturen, Verbindungsknoten, autarke Netze und Satellitenkommunikation können durch Quantenkryptographie geschützt werden. Mobile Datenübertragung und klassische Kommunikation werden die technisch simplere Post-Quanten-Kryptografie nutzen. Es bleibt aber nicht viel Zeit, um Strategien für die Gefahren von Morgen zu entwickeln. ■

Quantum Cybersecurity Group:
https://qscgroup.io