Deutscher Bundestag **Drucksache 19/18355**

19. Wahlperiode 24.03.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17500 –

Hochsicheres Quantennetzwerk QuNET

Vorbemerkung der Fragesteller

Ein zuverlässiges und abhörsicheres Netzwerk zur vertraulichen Kommunikation ist nach Auffassung der Fragesteller eine Grundvoraussetzung einer funktionierenden Demokratie. Zurzeit scheint die Quantenkommunikation, auf Grundlage quantentechnologischer Methodik oder Verfahren, ein vielversprechender Ansatz für ein eben solches sicheres Netz der Zukunft zu sein. Die Quantenkommunikation scheint beste Voraussetzungen für den Einsatz in hochsicheren Netzen zu bieten, da sich die Leitungen in einem solchen Netz nicht unbemerkt abhören lassen; wird ein Quant bei der Übertragung ausgelesen, so wird es zeitgleich unausweichlich verändert, sodass ein unerkanntes Mithören nicht möglich ist (https://www.spiegel.de/consent-a-?targetUrl=https%3A%2F%2Fwww.spiegel.de%2Fnetzwelt%2Fnetzpolitik%2Fquantenkommunikation-fraunhofer-baut-datenverbindung-fuer-ministerien-a-1301433.html). Es ist daher nicht verwunderlich, dass große Unternehmen (wie beispielsweise Google oder IBM) besonderes Interesse an diesem Bereich der Quantentechnologie zeigen und beträchtliche Summen in die entsprechende Forschung investieren (https://www.zdnet.de/88371751/ibm-vs-google-streit-um-quanten-vorherrschaft/).

Dies hat auch die Bundesregierung erkannt und über das Bundesministerium für Bildung und Forschung (BMBF) das Projekt „QuNET“ auf den Weg gebracht, um in Kooperation mit der Fraunhofer-Gesellschaft, der Max-Planck-Gesellschaft und dem Deutsche Zentrum für Luft- und Raumfahrt die Möglichkeiten der Quantentechnologie für die sichere Kommunikation (insbesondere zwischen Bundeseinrichtungen) auszuloten (https://www.bmbf.de/de/bmbf-initiative-qunet-baut-hochsicheres-quantennetzwerk-10126.html). Laut der Pressemitteilung des BMBF zum Start des Projekts soll es mehrere Projektphasen geben. Die erste Phase des Vorhabens bildet des „QuNET-alpha“, ein Demonstrationsexperiment zur Kommunikation unter Einsatz von Quantentechnologien. Weitere Phasen des Projekts zielen auf die Anschlussfähigkeit an europäische Quantennetz-Initiativen und den Aufbau einer deutschen Quantenkommunikationsinfrastruktur.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Bildung und Forschung vom 17. März 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Auf der Projektseite von „QuNET-alpha“ wird ein Projektvolumen in Höhe von 12,8 Mio. Euro bei einer Projektlaufzeit von 1Oktober 2019 bis Dezember 2020 angegeben (https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qunet-alpha). Zum Startschuss der Phase QuNET-alpha trafen sich die Mitglieder des Konsortiums am 12. November 2019 in Jena. Die Förderinitiative QuNET ist mit ihren drei Phasen auf eine Projektlaufzeit von sieben Jahren angelegt (https://www.hhi.fraunhofer.de/presse-medien/nachrichten/2019/startschuss-fuer-bmbf-initiative-qunet-fuer-abhoersichere-quantenkommunikation.html).

1. Wie ist nach Kenntnis der Bundesregierung der aktuelle Planungsstand des Projekts QuNET?

   a) Wie sieht der genaue Zeitplan für die geplanten drei Phasen aus?

   b) Welche Ziele bzw. Maßnahmen werden in den einzelnen Phasen jeweils konkret verfolgt?

Die Fragen 1 bis 1b werden gemeinsam beantwortet.

Das Projekt QuNET ist in drei Phasen unterteilt. In der ersten Phase, die von 2019 bis 2022 geplant ist, stehen neben der Demonstration einer quantengesicherten Videokonferenz zwischen zwei Bundeseinrichtungen die Umsetzung und Verlängerung von Punkt-zu-Punkt-Verbindungen im Mittelpunkt. In der zweiten Phase werden voraussichtlich von 2023 bis 2024 Technologien für Mehrbenutzer-Quantennetze entwickelt werden. Im Rahmen der dritten Phase werden voraussichtlich von 2025 bis 2026 konkrete Bausteine einer Quanteninfrastruktur entwickelt und die zuvor entwickelten Konzepte so skaliert werden, dass die Projektergebnisse auch in andere europäische Quantennetze integriert werden können.

Die Entwicklung einer Ende-zu-Ende verschlüsselten Quantenkommunikation ist ein unabdingbarer Baustein zukünftiger IT-Sicherheit. Die Quantenkommunikation ist entsprechend ein Schwerpunkt im Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“.

   c) Welche Bundesbehörden oder anderen Bundeseinrichtungen werden zu welchem Zeitpunkt beteiligt sein?

Derzeit wird QuNET in enger Abstimmung des Bundesministeriums für Bildung und Forschung (BMBF) mit dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt. Andere Ressorts werden in regelmäßigen Ressortbesprechungen über den aktuellen Stand von QuNET informiert, sodass eine Erweiterung der Beteiligten jederzeit möglich ist, sobald sich dies im Rahmen der Forschungs- und Entwicklungsarbeiten des Projekts bzw. für die erfolgreiche Verwertung der Projektergebnisse als sinnvoll und zielführend herausstellen sollte.

d) Sind neben der Fraunhofer-Gesellschaft, der Max-Planck-Gesellschaft und dem Deutsche Zentrum für Luft- und Raumfahrt weitere Partner beteiligt, oder ist geplant, künftig weitere Partner zu beteiligen?

In der Projektlaufzeit von QuNET ist geplant, neben den genannten Projektpartnern besonders qualifizierte Projektpartner aus Wissenschaft und Wirtschaft zu integrieren. Dies ermöglicht es einerseits, den hohen Risiken des Forschungs- und Entwicklungsvorhabens angemessen zu begegnen und das Know-how in Deutschland zu bündeln. Andererseits kann damit auch die Implementierung und Integration der neuen Technologien in bestehende Infrastrukturen mit ihren hohen Sicherheitsanforderungen beschleunigt werden. Ein Beirat mit Sicherheitsexperten und Vertretern aus der Wirtschaft begleitet die Arbeiten von QuNET und berät das Konsortium.

e) Mit welchen weiteren europäischen Quantennetz-Initiativen plant die Bundesregierung den Anschluss in den weiteren Projektphasen?

Welche europäischen Quantennetz-Initiativen existieren nach Kenntnis der Bundesregierung bereits?

Die Europäische Union bündelt die europäischen Quantennetz-Initiativen sowie vielfältige Initiativen der Mitgliedstaaten in der European Quantum Communication Infrastructure (QCI). Diese zielt langfristig auf ein die gesamte Europäische Union umfassendes Quantennetz ab. Derzeit nehmen bereits 24 der 27 Mitgliedstaaten teil. QuNET trägt einen essentiellen Teil zu einem künftigen Europäischen Quantennetzwerk bei, wodurch die Vorreiterrolle der Bundesrepublik Deutschland in der Entwicklung der technologieübergreifenden Quantenkommunikation gesichert und ausgebaut wird. Dies trägt nachhaltig zur Stärkung der technologischen Souveränität Deutschlands bei.

2. Wie ist der aktuelle Stand der Projektphase „QuNET-alpha“?

3. Wie sieht der genaue zeitliche Ablauf des Projekts aus?

4. Wann soll die avisierte „quantengesicherte Videokonferenz zwischen zwei Bundeseinrichtungen“ stattfinden (siehe https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qunet-alpha)?

5. Welche Bundeseinrichtungen sollen an der sicheren Videokonferenz teilnehmen?

Die Fragen 2 bis 5 werden gemeinsam beantwortet.

QuNET-alpha befindet sich aktuell in der technischen Umsetzung der Demonstrationsstrecke einer quantengesicherten Videokonferenz. Bislang wurden umfassende Systemkonzepte entwickelt und aufeinander abgestimmt. Es ist geplant, die Faser-, Freistrahl- und Satellitentechnologie in einem ganzheitlichen Systemdesign miteinander zu kombinieren. Derzeit prüft das BMBF in enger Zusammenarbeit mit dem BSI die technischen Rahmenbedingungen der Demonstrationsstrecke zwischen dem BMBF und einer weiteren Bundesbehörde. Die Demonstration der quantengesicherten Videokonferenz zwischen den beiden Bundesbehörden ist im vierten Quartal 2020 geplant.

6. Wie hoch ist das geplante finanzielle Gesamtvolumen für das Projekt QuNET insgesamt?

   a) Wie wird das finanzielle Gesamtvolumen über die Projektphasen verteilt?

Die Fragen 6 und 6a werden gemeinsam beantwortet

Aktuell ist ein Gesamtvolumen von 165 Mio. Euro für QuNET geplant. QuNET-alpha, bei dem es sich um den ersten Teil der ersten Projektphase handelt, wird mit insgesamt 12,8 Mio. Euro gefördert. Basierend auf den konkreten Forschungs- und Entwicklungsergebnissen von QuNET-alpha wird die Projekt-, Zeit- und Finanzplanung von QuNET weiter ausgearbeitet werden. Dies beinhaltet auch die Aufteilung der Finanzmittel über die weiteren Projektphasen.

   b) Ist das Projekt QuNET Teil der von der Bundesregierung in der aktuellen Legislaturperiode für die Erforschung der Quantentechnologien bereitgestellten 650 Mio. Euro (https://www.quantentechnologien.de/index.html)?

Das Rahmenprogramm der Bundesregierung zur Erforschung der Quantentechnologien bündelt als Dachstrategie die unterschiedlichen Maßnahmen der Ressorts sowie unterschiedlicher Förderprogramme. Dazu zählt auch die Quantenkommunikation, die ein wichtiger Förderschwerpunkt im Forschungsrahmenprogramm der Bundesregierung für IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“ ist. Das Forschungs- und Entwicklungsvorhaben QuNET ist darin verankert und trägt so auch zur Hightech-Strategie 2025 der Bundesregierung bei. QuNET-alpha ist Teil der für die aktuelle Legislaturperiode vorgesehenen Aktivitäten. Das Projekt QuNET erstreckt sich jedoch über die Legislaturperiode hinaus.

7. Wie ist nach Kenntnis der Bundesregierung der aktuelle Entwicklungsstand bei Quantenrepeatern?

   Wann ist nach Einschätzung der Bundesregierung mit einem möglichen Einsatz in der Kommunikationsinfrastruktur des Bundes zu rechnen?

Das BMBF fördert seit 2010 die Erforschung und Entwicklung von Quantenrepeatern. Es ist davon auszugehen, dass als Ergebnis des Forschungsprojekts Q.Link.X Mitte 2021 der erste Quantenrepeaterknoten als funktionsfähiger Labordemonstrator verfügbar sein wird. Solche Knoten werden die elementaren Bausteine von künftigen Quantenrepeaternetzen darstellen. Sobald die Forschungsergebnisse aus Q.Link.X vorliegen, wird festgelegt, wann diese in die Arbeiten in QuNET einfließen werden.

8. Welche Bundesbehörden oder anderen Bundeseinrichtungen sollen an das geplante Behördennetzwerk auf Basis von Quantentechnologie angeschlossen werden?

Bei QuNET handelt es sich um ein Forschungs- und Entwicklungsprojekt, das der anwendungsorientierten Grundlagenforschung zuzuordnen ist. Angesichts der dementsprechend hohen technischen Unwägbarkeiten des Vorhabens ist die weitere Detaillierung maßgeblich vom Projektverlauf abhängig. Die Entscheidung, wann welche Bundesbehörde oder -einrichtung an das neuartige Quantennetz angeschlossen werden kann, hängt maßgeblich vom Grad der Implementierbarkeit der Projektergebnisse in die Infrastrukturen der einzelnen Behörden bzw. Einrichtungen ab. Erste Erkenntnisse werden diesbezüglich bereits bei der Umsetzung der Demonstrationsstrecke im Rahmen von QuNET-alpha gewonnen werden. Ergänzend wird auf die Antwort zu Frage 1c verwiesen.

9. Sieht die Bundesregierung Netzwerke auf Basis von Quantentechnologie generell als „Zukunft der IT-Sicherheit“ an?

   a) Falls ja, wie soll bis zur flächendeckenden Einführung eines Netzwerkes auf Basis von Quantentechnologie die Sicherheit von kritischen Netzen im Zuständigkeitsbereich der Bundesregierung gegenüber bereits entwickelten oder in Entwicklung befindliche Quantencomputern sichergestellt werden?

   b) Falls nein, wie soll die Sicherheit von kritischen Netzen im Zuständigkeitsbereich der Bundesregierung anderweitig gegenüber bereits entwickelten oder in Entwicklung befindlichen Quantencomputern sichergestellt werden?

Die Fragen 9 bis 9b werden gemeinsam beantwortet.

Quantentechnologie ist lediglich für Teilaspekte von Netzwerksicherheit eine Lösungsmöglichkeit, insbesondere für sicheren Schlüsselaustausch. Daher setzt die Bundesregierung auf den Einsatz von quantencomputerresistenten Public-Key-Verschlüsselungs- und -Signaturverfahren, sogenannten Postkryptografieverfahren. Diese sind universell einsetzbar, da sie auf der aktuell verfügbaren Informations- und Kommunikationsinfrastruktur aufsetzen und die Sicherheit von kritischen Netzen gewährleisten. Die Sicherheit dieser Verfahren wird nach jetzigem Kenntnisstand nicht durch Quantencomputer eingeschränkt. Parallel zu der zielgerichteten Förderung der anwendungsnahen Grundlagenforschung und Technologieentwicklungen im Bereich der Quantenkommunikation werden daher im Rahmen des aktuellen Forschungsrahmenprogramms für IT-Sicherheit zahlreiche Aktivitäten im Bereich der Postquantenkryptographie durchgeführt. Damit wird ein Bereich gefördert, der die Übergangszeit bis zur Verfügbarkeit von Quantenkommunikationssystemen überbrücken soll und darüber hinaus die Quantenkommunikationsinfrastruktur als komplementäre Technologie zur Absicherung vor Angriffen mit Quantencomputern ergänzt.

In Produkten für den Hochsicherheitsbereich setzt das BSI bereits Maßnahmen ein, die das Risiko durch Angriffe mit Quantencomputern verringern. Diese Maßnahmen werden aktuell um quantencomputerresistente Public-Key-Verschlüsselungs- und -Signaturverfahren erweitert. Die kommende Ausgabe der technischen Richtlinie des BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ wird Empfehlungen zu diesen Verfahren enthalten. Ergänzend wird auf die Antwort zu Frage 10b verwiesen.

10. Inwiefern wird die allgemeine Entwicklung von Quantentechnologie nach Ansicht der Bundesregierung Auswirkungen auf die Gesellschaft haben?

    a) Wann ist nach Ansicht der Bundesregierung mit einer Beeinträchtigung der digitalen Sicherheit der Bürgerinnen und Bürger zu rechnen (beispielsweise durch signifikant effizienteres Überwinden von Passwörtern durch Quantencomputer)?

Die Fragen 10 und 10a werden gemeinsam beantwortet.

Handlungsbedarf ergibt sich zunächst für Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten. Hier besteht die Gefahr darin, dass verschlüsselte Daten auf Vorrat gesammelt und in der Zukunft mit Hilfe eines Quantencomputers entschlüsselt werden könnten (allgemein bekannt als „store now, decrypt later"-Szenario).

Quantencomputer sind nach jetzigem Kenntnisstand nicht in der Lage, signifikant effizientere Angriffe auf nach Stand der Technik gesicherte Passwörter durchzuführen. Für detailliertere Informationen verweist die Bundesregierung auf eine Studie des BSI zu dieser Thematik, die unter www.bsi.bund.de/qcst udie abgerufen werden kann.

    b) Wie soll nach Ansicht der Bundesregierung auch im Postquantenzeitalter der digitale Schutz der Bürgerinnen und Bürger sichergestellt werden?

Es existieren grundsätzlich zwei Lösungsansätze, um den digitalen Schutz der Bürgerinnen und Bürger sicherzustellen:

Ein potentieller Lösungsansatz ist die im QuNET-Projekt geplante Quantenkommunikation. Hierbei arbeitet das BSI an der Erstellung von Prüfkriterien für die Bewertung der Sicherheit von Produkten zur Quantenkommunikation. Die Quantenkommunikation ist wegen technischer Einschränkungen nur in ausgewählten Szenarien (z. B. Telekommunikations-Backbones) denkbar, bietet derzeit keine Ende-zu-Ende-Sicherheit und benötigt darüber hinaus einen authentischen Kommunikationskanal (z. B. mittels quantencomputerresistenten Public-Key-Signaturverfahren). Mit den aktuellen gezielten BMBF-Förderinitiativen zu dieser Technologie (z. B. QuNET, Q.Link.X) sollen diese Einschränkungen überwunden werden, sodass die Quantenkommunikation als wichtiger Baustein die digitale Sicherheit der Bürgerinnen und Bürger nachhaltig stärken kann. Im internationalen Vergleich nimmt Deutschland im Bereich der Quantenkommunikation eine führende Rolle ein.

Der zweite Lösungsansatz ist die Umstellung der gegenwärtig verwendeten Public-Key-Verschlüsselungs- und -Signaturverfahren auf solche, die als resistent gegenüber Angriffen mittels Quantencomputern gelten (Postquantenkryptografie). Solche Public-Key-Verfahren durchlaufen derzeit einen Auswahlprozess des amerikanischen National Institute of Standards and Technology (NIST), der vom BSI eng begleitet wird. So kann auch die derzeit genutzte Informations- und Kommunikationsinfrastruktur trotz möglicher Angriffe durch Quantencomputer sicher verwendet werden.

Hinsichtlich der Sicherheitsbedrohung, die von künftigen anwendungstauglichen Quantencomputern ausgeht, befinden sich Maßnahmen wie beispielsweise die fokussierte Förderung der Entwicklung von Postquantenkryptografie-Methoden bereits in der Umsetzung. In diesem Bereich fördert das BMBF im Forschungsrahmenprogramm der Bundesregierung für IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt" aktuell Forschungs- und Entwicklungsvorhaben mit insgesamt etwa 16 Mio. Euro.

Die beiden Lösungsansätze beruhen auf komplementären Technologien. Mit der zielorientierten Weiterführung der aktuellen Forschungs- und Entwicklungsarbeiten beider Ansätze wird die digitale Sicherheit der Bürgerinnen und Bürger nachhaltig gestärkt.

11. Haben andere Staaten und/oder Organisationen nach Kenntnis der Bundesregierung bereits Kommunikationsnetzwerke auf Basis von Quantentechnologie im Einsatz?

    a) Falls ja, um welche Staaten und/oder Organisationen handelt es sich hierbei, und inwiefern haben diese ein solches Kommunikationsnetzwerk implementiert?

    b) Falls nein, welche Staaten und/oder Organisationen entwickeln nach Kenntnis der Bundesregierung momentan ein solches Kommunikationsnetzwerk auf Basis von Quantentechnologie, und wie weit ist die Entwicklung jeweils fortgeschritten?

Die Fragen 11 bis 11b werden gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung existieren aktuell weltweit verschiedene Test- und Demonstrationsstrecken, die auf Quantentechnologien basieren. Beispiele hierfür sind unter anderem in China, Großbritannien, Kanada, Österreich und den Niederlanden zu finden. Hierbei handelt es sich jedoch nicht um Ende-zu-Ende quantenverschlüsselte Netzwerke für mehrere Teilnehmer, wie sie mit den in QuNET zu entwickelnden Technologien angestrebt sind. So ist beispielsweise im Rahmen der Trusted-Node-Strecke in China keine vollständige Ende-zu-Ende-Verschlüsselung realisiert worden, sondern nur Teilstrecken sind quantengesichert.

12. Welche Sicherheitsvorteile bietet ein Netzwerk auf Basis von Quantentechnologie nach Kenntnis der Bundesregierung im Vergleich zu aktuell als sicher geltenden Netzwerken?

Die Sicherheit der meisten aktuell als sicher geltenden Netzwerke, die auf komplexen Algorithmen basiert, ist durch die technologischen Fortschritte der verfügbaren Quantencomputer entscheidend bedroht. Die extrem hohe Leistungsfähigkeit dieser neuartigen Rechner wird es künftig ermöglichen, den Schutz der derzeit gängigen Verschlüsselungsmethoden zu überwinden. Auch jetzt könnten bereits verschlüsselte Übertragungen abgehört und gespeichert werden, um diese mit einem zukünftigen Quantencomputer zu entschlüsseln.

Die Sicherheit der Quantenkommunikation beruht hingegen auf physikalischen Grundprinzipien, die durch keinen noch so leistungsfähigen Rechner überwunden oder umgangen werden können. Mit einem vollständig Ende-zu-Ende-verschlüsselten quantengesicherten Netzwerk wird daher erstmals eine Netzwerk-Infrastruktur geschaffen, die eine langfristig nachhaltige – und von der Entwicklung von Super- oder Quantencomputern unabhängige – Datensicherheit ermöglicht.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333