Deutscher Bundestag **Drucksache 20/8104**

20. Wahlperiode 23.08.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Edgar Naujok, Barbara Lenk, Eugen Schmidt, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 20/7985 –

Quantentechnologie und deren Anwendung zu Spionage- und Sabotagezwecken

Vorbemerkung der Fragesteller

Hinsichtlich der Ausspähungsgefahr mittels Quantentechnologie empfahl die Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS) in einer Stellungnahme vom 18. Januar 2023, die „[w]issenschaftliche Forschung im Bereich neuer quantensicherer kryptographischer Verfahren“ zu verstärken. Ebenso empfahl sie „dem Staat eine stringente Umsetzung und Rechtsdurchsetzung von Prinzipien des security-by-design und privacy-by-design“ (www.bundestag.de/resource/blob/929948/d607e3604be4c777cd8186265a912386/Stellungnahme-Atug-data.pdf, S. 23). Dementsprechend ist nach Ansicht der Fragesteller zu klären, inwiefern das vom Bundesverfassungsgericht (BVerfGE) 2008 formulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274) berührt ist.

Bezüglich des Gefährdungspotenzials durch Quantencomputer prognostiziert die Technische Universität Kaiserslautern, dass aufgrund der rapiden Entschlüsselungsgeschwindigkeit kritische Infrastrukturen wie etwa die Energieversorgung durch Hacker sabotiert werden können (Vgl. idw-online.de/de/news761213). Auch IT-Sicherheitsunternehmen warnen davor, dass weltweit die Sicherheitssysteme nicht auf die immense Rechenleistungsfähigkeit der Quantencomputer vorbereitet seien (www.focus.de/magazin/archiv/agenda-krieg-der-hacker_id_191705434.html). Aus Sicht der Fragesteller ist daher zum Beispiel zu klären, ob bei der möglichen Ausspähung des Bundesministeriums der Verteidigung (BMVg) durch US-amerikanische Geheimdienste im April 2023 Quantentechnologie zum Einsatz kam (www.zeit.de/politik/2023-04/pentagon-leaks-ueberwachung-bundesverteidigungsministerium).

Es ist aus Sicht der Fragesteller dringend geboten, dass die Bundesregierung mögliche Mängel bei dem Schutz von Bevölkerung, staatlichen Institutionen und wirtschaftlichen Akteuren durch negative Auswirkungen der Quantentechnologie darlegt sowie ihre Bestrebungen schildert, damit umzugehen. Dabei sind etwa Fragen der Rechtsdurchsetzung von elementarer Bedeutung.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 22. August 2023 übermittelt.

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

Vorbemerkung der Bundesregierung

Quantentechnologien wie Quantencomputing und Quantenkommunikation sind Zukunftstechnologien mit disruptivem Potenzial und besonders vielversprechenden Anwendungsperspektiven. Obwohl sie sich noch in einem vergleichsweise frühen Entwicklungsstadium befinden, zeichnen sich bereits jetzt innovative Nutzungsmöglichkeiten in Wirtschaft und Gesellschaft ab. Sie werden aber auch massive Auswirkungen auf die Informationssicherheit haben.

Aus Sicht der IT-Sicherheit stellt die Entwicklung von leistungsfähigen Quantencomputern eine Bedrohung dar: Der so genannte Shor-Algorithmus, ein Verfahren der Quanteninformatik, wäre in der Lage, die heute eingesetzte Public-Key-Kryptografie zu brechen. Noch existiert die dafür nötige Quantencomputing-Hardware nicht. Sobald diese jedoch verfügbar ist, würde dies ein großes Risiko darstellen, da derzeit mit solchen Verschlüsselungsverfahren vertrauliche Kommunikation und sicherheitsrelevante Daten abgesichert werden. Schon jetzt könnten verschlüsselte Daten abgehört und aufgezeichnet werden, um mit künftigen Quantencomputern entschlüsselt zu werden ("store now, decrypt later").

Dies macht die Entwicklung und Einführung neuer, quantensicherer kryptografischer Verfahren ("Post-Quanten-Kryptografie") zwingend erforderlich, die gegenüber Quantencomputern eine mindestens ebenso hohe Sicherheit bieten sollen wie die oben genannten klassischen Verfahren heute. Weitere Informationen dazu finden sich beispielsweise in dem Leitfaden „Kryptografie quantensicher gestalten“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (bsi.bund.de/PQ-Migration).

Die Notwendigkeit der Migration zu Post-Quanten-Kryptografie in Deutschland wird auch im „Handlungskonzept Quantentechnologien“ der Bundesregierung angesprochen (dserver.bundestag.de/btd/20/066/2006610.pdf). Ziel der Bundesregierung ist, bis 2026 eine Strategie zur Migration zu Post-Quanten-Kryptografie in Deutschland zu erstellen.

Ab wann Quantencomputer tatsächlich in der Lage sein werden, kryptografische Verfahren zu brechen, lässt sich nicht pauschal beantworten. Im staatlichen Hochsicherheitsbereich wird unter der Hypothese gearbeitet, dass Anfang der 2030er Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen werden (dserver.bundestag.de/btd/19/252/1925208.pdf). Diese Aussage ist nicht als Prognose zur Verfügbarkeit von Quantencomputern zu verstehen, sondern stellt einen Richtwert für die Risikobewertung dar. Eine ausführliche Studie zum „Entwicklungsstand Quantencomputer“ wurde vom BSI veröffentlicht (bsi.bund.de/qcstudie). Diese Studie wird regelmäßig aktualisiert.

1. Sieht die Bundesregierung im Hinblick auf negative Auswirkungen von Quantentechnologie Grundrechte deutscher Staatsbürger gefährdet, und wenn ja, welche, und in welcher Weise, und welchen gesetzgeberischen Handlungsbedarf zieht sie ggf. hieraus?

23. Hat die Bundesregierung Kenntnis von einer möglichen Bedrohung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch die missbräuchliche Anwendung von Quantentechnologie, und wenn ja, mit welchen Mitteln will sie die Rechtsdurchsetzung dahingehend stärken?

30. Sieht die Bundesregierung derzeit das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgrund einer möglichen Ausspähung mittels Quantentechnologie gefährdet, und wenn ja, mit welchen gesetzgeberischen und weiteren Maßnahmen will sie ggf. darauf reagieren?

Die Fragen 1, 23 und 30 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Einer möglichen künftigen Gefährdungslage begegnet die Bundesregierung im Handlungskonzept Quantentechnologien. Konkret wird darin die „Erstellung einer Strategie der Bundesregierung zur Migration zur Post-Quanten-Kryptografie“ als Ziel für 2026 genannt.

2. Inwiefern ist die Bundesregierung bestrebt, mit der Entwicklung von Quantentechnologie die Sicherheit vor Ausspähaktionen gegenüber deutschen Behörden sowie deutschen Staatsbürgern und Unternehmen zu erhöhen, und wie will sie dieses Ziel bis wann erreichen?

Im Rahmen des Forschungsrahmenprogramms „Digital.Sicher.Souverän.“, setzt die Bundesregierung die Unterstützung der Forschung in der IT-Sicherheit fort und stärkt insbesondere den Transfer von der Wissenschaft zur Wirtschaft. Hierdurch soll die technologische Souveränität Deutschlands und damit die IT-Sicherheit der Bürgerinnen und Bürger gesteigert werden. Die Forschungsförderung des Bundesministeriums für Bildung und Forschung (BMBF) zur Quantenkommunikation und Post-Quanten-Kryptografie nimmt eine zentrale Rolle an der Schnittstelle zu den klassischen Kommunikationstechnologien ein und dient dem langfristigen Schutz gegen mögliche Ausspähaktionen, auch im Zeitalter des Quantencomputers. Diese und weitere Maßnahmen und Ziele sind darüber hinaus im „Handlungskonzept Quantentechnologien“ der Bundesregierung dargelegt und sollen bis 2026 perspektivisch erreicht werden.

3. An welche „Fragen der inneren und äußeren Sicherheit“ im Einzelnen denkt die Bundesregierung im Rahmen ihres Handlungskonzeptes Quantentechnologie, und welchen gestalterischen Anspruch verfolgt sie hierbei (www.bmbf.de/SharedDocs/Downloads/de/2023/230426-handlungskonzept-quantentechnologien.pdf?__blob=publicationFile&v=3, S. 24)?

Wie in der Vorbemerkung der Bundesregierung dargestellt, bieten Quantentechnologien sowohl Chancen aber vor allem auch Risiken für die Cybersicherheit. In diesem Sinne ist die zitierte Aussage im Handlungskonzept als allgemeiner Hinweis zu verstehen.

4. Beabsichtigt die Bundesregierung, auf den Einsatz von Quantentechnologie etwa in Verbindung mit künstlicher Intelligenz zur Bekämpfung der irregulären Migration hinzuwirken, und wenn ja, in welcher Weise, wenn nein, warum nicht?

Die Bundesregierung befindet sich zum Thema Einsatz von Quantentechnologie zur Verhinderung irregulärer Migration, auch in Verbindung mit Künstlicher Intelligenz, gegenwärtig in Abstimmung.

5. Hat die Bundesregierung Kenntnis von quantentechnologischen Anwendungen aus dem Ausland – insbesondere aus auf S. 2 des Handlungskonzepts erwähnten konkurrierenden Ländern –, welche die Informationssicherheit und den Datenschutz in Deutschland bedrohen, und wenn ja, welche sind dies?

Wie in der Vorbemerkung der Bundesregierung dargestellt, sind die Informationssicherheit und der Datenschutz potentiell zukünftig durch die Ausnutzung von Quantentechnologien gefährdet. Dies schließt auch quantentechnologische Anwendungen aus dem Ausland mit ein.

6. Inwiefern ist die Bundesregierung grundsätzlich bereit, Transparenz für die Öffentlichkeit hinsichtlich möglicher Bedrohungen mittels Quantentechnologie herzustellen, und in welcher Form gedenkt sie dies ggf. zu tun?

Das BSI informiert die Öffentlichkeit in Veröffentlichungen und in Vorträgen auf zahlreichen Veranstaltungen über die Bedrohungen durch Quantentechnologien für die Cybersicherheit. Entsprechend dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme nimmt das BSI unter anderem die Aufgabe wahr, „Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen" (§ 3 Nummer 14) zu beraten, zu informieren und zu warnen. Dies schließt explizit Verbraucherinnen und Verbraucher ein (siehe § 3 Nummer 14a). Damit sind auch mögliche Bedrohungen durch Quantentechnologie von dieser Maßgabe eingeschlossen. Das BSI kommt dem, falls nötig, mittels unterschiedlichster Kommunikationsmaßnahmen nach. Dazu gehören exemplarisch die Information der Öffentlichkeit über Presseinformationen, durch Soziale Medien und Veröffentlichung auf den Webseiten des BSI. Insbesondere informiert das BSI auf seiner Webseite zu den aktuellen Entwicklungen im Bereich Quantentechnologie und Post-Quanten-Kryptografie (bsi.bund.de/Quanten).

7. Wie schätzt die Bundesregierung die gegenwärtige Bedrohungslage durch Ausspähung mittels Quantentechnologie durch Drittstaaten ein?

12. Hält die Bundesregierung die gegenwärtigen Maßnahmen und Sicherheitsstandards für angemessen und ausreichend, um potenzielle Ausspähmaßnahmen mittels Quantentechnologie abzuwehren bzw. nachzuvollziehen?

17. Hat die Bundesregierung Kenntnis von möglichen versuchten und erfolgten Angriffen auf kritische Infrastruktur mittels Quantentechnologie in Deutschland, und wenn ja, wie viele waren dies in den Jahren 2021 und 2022?

Die Fragen 7, 12 und 17 werden gemeinsam beantwortet.

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 7, 12, 17, 18 und 29 zur gegenwärtigen Bedrohungslage durch Quantentechnologien und entsprechende mögliche Abwehrmaßnahmen aufgrund entgegenstehender überwiegender Belange des Staatswohls nicht erfolgen kann, auch nicht in eingestufter Form. Eine Antwort der Bundesregierung auf die Frage, ob eine Bedrohungslage vorliegt und welche Strukturen zur Abwehr bestehen könnten, würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen

Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass mögliche operative Fähigkeiten und Methoden aufgeklärt und damit die Arbeitsweise der Sicherheitsbehörden gefährdet würde. Denn eine Beantwortung der Frage ließe Rückschlüsse auf deren eventuelle Kenntnisstände zu Bedrohungslagen sowie entsprechender Sicherheitsstandards und Abwehrmaßnahmen zu. Dies wäre insbesondere der Fall, wenn vermehrt anlassbezogen zu möglichen einzelnen Maßnahmen gefragt wird. Letztendlich könnte dies dazu führen, dass ein Großteil der Fähigkeiten und Kenntnisstände der Sicherheitsbehörden, nicht nur zu Quantentechnologien, sondern auch zu weitergehender Ausstattung und Fähigkeiten, der breiten Öffentlichkeit bekannt wird. Es könnten entsprechende Abwehrstrategien und Angriffsmöglichkeiten entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland bedeuten. Aus der sorgfältigen Abwägung der verfassungsrechtlich garantierten Informationsrechte des Deutschen Bundestages und seiner Abgeordneten mit den negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung der deutschen Sicherheitsbehörden sowie den daraus resultierenden Beeinträchtigungen der Sicherheit der Bundesrepublik Deutschland folgt, dass auch eine Auskunft nach Maßgabe der Geheimschutzordnung und damit einhergehende Einsichtnahme über die Geheimschutzstelle des Deutschen Bundestages ausscheidet. Hierbei würde wegen der großen Anzahl der Geheimnisträger die Wahrscheinlichkeit erhöht, dass die mitgeteilten Informationen ausgespäht werden. Die vorliegend erfragten Informationen sind aus Sicht der Bundesregierung, wie voranstehend dargelegt, in derart hohem Maße geheimhaltungsbedürftig, dass auch in Ansehung der vom Bundestag ergriffenen Geheimschutzmaßnahmen ein verbleibendes geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann, so dass ausnahmsweise das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt und die Bundesregierung aus diesen Gründen von einer Beantwortung absehen kann (vgl. Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 124, 78 [124 ff., 139]).

8. Haben die Bundesregierung bzw. nachgeordnete Sicherheitsbehörden bereits versuchte und erfolgte Ausspähmaßnahmen mittels Quantentechnologie registriert, und wenn ja, welche sind dies (bitte auflisten)?

13. Hat die Bundesregierung Kenntnis, ob Quantentechnologie im Kontext des Ukraine-Krieges Anwendung findet, und wenn ja, in welcher Weise?

19. Als wie groß sieht die Bundesregierung die gegenwärtige Gefahr der Sabotage kritischer Infrastruktur mittels Quantentechnologie durch fremde staatliche und nichtstaatliche Akteure?

Die Fragen 8, 13 und 19 werden gemeinsam beantwortet.

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass eine Beantwortung der Fragen 8, 13, 18, 19 und 29 zur gegenwärtigen Bedrohungslage aufgrund entgegenstehender überwiegender Belange des Staatswohls nicht erfolgen kann, auch nicht in eingestufter Form. Die erfragten Informationen zielen im Kern auf die Offenlegung bestimmter nachrichtendienstlicher Arbeitsmethoden und Vorgehensweisen im Bereich der technischen Aufklärung. Solche Arbeitsmethoden sind im Hinblick auf die künftige Erfüllung des gesetzlichen Auftrages der betroffenen Nachrichtendienste jedoch besonders schutzwürdig. Der Schutz der technischen Aufklärungsfähigkeiten stellt für die Aufgabenerfüllung der Nachrichtendienste einen überragend wichtigen Grundsatz dar. Er dient der Aufrechterhaltung der Effektivität nachrich-

tendienstlicher Informationsbeschaffung durch den Einsatz spezifischer technischer Fähigkeiten und damit dem Staatswohl. Das Bekanntwerden der näheren Umstände der technischen Aufklärungsfähigkeiten, Tätigkeiten und Analysemethoden könnte das Wohl des Bundes gefährden. Eine Antwort der Bundesregierung würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die Fragestellung berührt derart schutzbedürftige Geheimhaltungsinteresse, dass auch ein geringfügiges Risiko des Bekanntwerdens, wie es auch bei einer Übermittlung an die Geheimschutzstelle des Deutschen Bundestages nicht ausgeschlossen werden kann, aus Staatswohlgründen vermieden werden muss. In diesem überwiegt daher das Staatswohlinteresse gegenüber dem parlamentarischen Informationsrecht.

9. Sind der Bundesregierung die Anlässe und Beweggründe möglicher Ausspähmaßnahmen bekannt, und wenn ja, welche sind dies?

10. Sieht die Bundesregierung spezifische Bereiche der öffentlichen Sektoren und der kritischen Infrastruktur besonders anfällig für die Ausspähung mittels Quantentechnologie, und wenn ja, welche sind dies?

Die Fragen 9 und 10 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet:

Die Anlässe und Beweggründe möglicher Ausspähmaßnahmen bewegen sich, losgelöst vom Einsatz eines technischen Mittels, entlang des jeweiligen Interessen- und Auftragsprofils eines ausländischen Nachrichtendienstes (AND) und orientieren sich an den nachrichtendienstlichen Abwehrmechanismen, denen sich der jeweilige AND gegenübersieht. Der Einsatz besonders leistungsstarker Rechner steht insbesondere dann zu erwarten, wenn ein AND besonders komplexe, technische Sicherheitsmaßnahmen zu umgehen sucht.

11. Will die Bundesregierung bestimmte öffentlicher Sektoren und Bereiche der kritischen Infrastruktur besonders vor der Ausspähung mittels Quantentechnologie schützen, und wenn ja, welche sind dies, und in welcher Weise will sie dies erreichen?

Die Bundesregierung und insbesondere das BSI unterstützt die Eigenverantwortung der Betreiber Kritischer Infrastrukturen durch einen ganzheitlichen Ansatz (Prävention, Detektion, Reaktion). Diese halten ein angemessenes Niveau an IT-Sicherheit vor, welches regelmäßig durch Dritte geprüft wird. Im Falle der konkreten Kenntnis von Schwachstellen, Angriffsversuchen oder weiteren Erkenntnissen warnt das BSI Betreiber Kritischer Infrastrukturen und empfiehlt zugleich Maßnahmen zur Abwehr bzw. Mitigation.

14. Aus welchen Gründen wurde für die im Kontext der Quantentechnologie erwähnte Cybersicherheitsstrategie ein Handlungszeitraum von fünf Jahren angelegt, und anhand welcher Indikatoren erfolgte diese Bemessung (www.bmbf.de/SharedDocs/Downloads/de/2023/230426-handlungskonzept-quantentechnologien.pdf?__blob=publicationFile&v=3, S. 31)?

Im Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP wurde vereinbart, dass die „Cybersicherheitsstrategie für Deutschland 2021“ weiterentwickelt wird. Der Prozess dauert derzeit an.

15. Kann aus dem Verweis der Bundesregierung im Handlungskonzept Quantentechnologien auf den Ukraine-Krieg geschlossen werden, dass die Bundesregierung einen Zusammenhang zwischen der Bedrohung der technologischen Souveränität und dem Krieg in der Ukraine sieht, und wenn ja, in welcher Weise ist dies ihrer Ansicht nach der Fall (ebd., S. 20)?

Die COVID-19-Pandemie sowie der Ukrainekrieg wurden im Handlungskonzept als aktuelle Beispiele für exogene Auslöser von allseits bekannten Störungen der globalen Lieferketten genannt. Damit ist keine konkretisierte Bedrohung der technologischen Souveränität Deutschlands gemeint. Gleichwohl können kriegsbedingte Produktionsausfälle in der Ukraine bei bestimmten Stoffen, bei denen das Land einen signifikanten Weltmarktanteil aufweist, auch negative Auswirkungen auf die nachgelagerte Hochtechnologiestufen in Deutschland entfalten (z. B. Neongas für Halbleiterherstellung).

16. Sieht die Bundesregierung die Souveränität Deutschlands potenziell durch den Einsatz von quantentechnologiebasierter Ausspähung durch Drittstaaten gefährdet, und wenn ja, in welcher Weise?

Wie in der Vorbemerkung der Bundesregierung dargestellt, sind die Cybersicherheit und damit auch die digitale Souveränität der Bundesrepublik Deutschlands potentiell zukünftig durch die Ausnutzung von Quantentechnologien gefährdet.

18. Hat die Bundesregierung davon Kenntnis, ob es Versuche von anderen Staaten bzw. von nichtstaatlichen Akteuren gibt, die bis 2026 angestrebte Entwicklung eines Quantencomputers zu sabotieren, und wenn ja, wie begegnet sie diesen?

Es wird auf die Antworten zu den Fragen 7 und 8 verwiesen.

20. Als wie groß sieht die Bundesregierung die gegenwärtige Gefahr der Ausspähung von Gesundheitsdaten deutscher Staatsbürger mittels Quantentechnologie, und gedenkt sie, gerade in diese grundrechtssensiblen Bereich die Sicherheitsstandards zu erhöhen, und wenn ja, in welcher Weise?

Der Bundesregierung sind keine Angriffe mittels Quantentechnologie auf die Vertraulichkeit von Gesundheitsdaten bekannt. Im Rahmen der Fortentwicklung der Telematikinfrastruktur wird die Möglichkeit geprüft, kryptografische Verfahren auf Post-Quanten-Kryptografie umzustellen.

21. Hat die Bundesregierung Kenntnis vom aktuellen Stand der Entwicklung quantensicherer kryptographischer Verfahren in Deutschland, und wenn ja, wie bewertet sie diesen im europäischen und internationalen Vergleich?

Aktuell ist die Bundesrepublik Deutschland im internationalen Vergleich im Bereich der Forschung und Entwicklung zur Quantenkommunikation und der Post-Quanten-Kryptografie gut aufgestellt. Das BSI hat frühzeitig erste Empfehlungen zur Migration zu Post-Quanten-Kryptografie gemacht (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html?nn=129156). Die Bundesrepublik Deutschland verfügt zudem über internationale führende Forschergruppen sowohl in der Erforschung des glasfaserbasierten Quantenschlüsselaustausches als auch in deren Übertragung per Satellit. Erste Quantenkommunikationsprodukte werden bereits angeboten.

22. Hat die Bundesregierung die von der Arbeitsgemeinschaft Kritische Infrastrukturen empfohlene Würdigung und Anwendung von security-by-design und privacy-by-design zur Kenntnis genommen, und wenn ja, in welcher Weise verfolgt sie diese, und wie will sie möglichen Herausforderungen hierbei begegnen?

IT-Sicherheit ist als Anforderung an moderne IT-Produkte etabliert und wird weitestgehend in den Entwicklungsprozess relevanter Hersteller über den Lebenszyklus der Produkte integriert. Mittels Technischer Richtlinien werden Sicherheitsanforderungen durch das BSI veröffentlicht und finden in den Entwicklungsprozessen Berücksichtigung. Darüber hinaus fordert und fördert das BSI sowohl security-by-design als auch privacy-by-design als Prinzipien, über Einzelempfehlungen von Arbeitsgemeinschaften hinaus. Kürzlich hat das BSI bspw. gemeinsam mit internationalen Partnerbehörden eine Handreichung zum Thema an IT-Hersteller veröffentlicht. Siehe: www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230413_CISA-Handreichung.html.

24. Hat die Bundesregierung Kenntnis von volkswirtschaftlichen Schäden infolge von möglichen Hackerangriffen mittels Quantentechnologie auf kritische Infrastrukturen und weitere Einrichtungen, und wenn ja, wie hoch beziffert sie diese (bitte ggf. auffschlüsseln)?

Wie in der Vorbemerkung der Bundesregierung dargestellt, sind Quantentechnologien zurzeit noch keine Bedrohung für die IT-Sicherheit.

25. Wie bewertet die Bundesregierung den aktuellen Stand des Projekts „Post-Quanten-sichere Kommunikation für die Industrie 4.0“, und welche Erfolge konnten hierbei aus ihrer Sicht bereits erzielt werden?

Das Projekt „Post-Quanten-sichere Kommunikation für die Industrie 4.0“ (PoQsiKom) entwickelt eine der wesentlichen Grundlagen, um die sichere, souveräne und effiziente Vernetzung der Betriebstechnik in der Industrie 4.0 langfristig zu ermöglichen und damit ein hohes Maß an Interoperabilität zu gewährleisten. Ziel des Projektes ist die Härtung von Edge Devices und Komponenten der Betriebstechnik für ein gesteigertes Sicherheitsniveau, welches auch den kryptographischen Fähigkeiten von Quantencomputer gewachsen ist. Das Projekt liegt nach etwas über einem Jahr Projektlaufzeit im Plan und konnte bereits erste Ergebnisse präsentieren.

26. Hält es die Bundesregierung für realistisch, dass bis zum Laufzeitende des Projekts am 30. November 2024 eine umfängliche Sicherheit für Anwendungen von Industrie 4.0 gewährleistet sein wird, und wenn ja, anhand welcher Indikatoren wird sie dies festmachen?

Das Ziel des Forschungsprojekts ist die praktische Umsetzung der Forschungsergebnisse in einem industriellen Demonstrator. Darüber hinaus wird als weitere, benötigte Komponente ein Echtzeitbetriebssystem für die vorgesehenen Anwendungsfälle technisch gehärtet. Das Gesamtvorhaben kooperiert mit einem Schwesterprojekt in Korea und strebt eine internationale Standardisierung der Ergebnisse an.

27. Aus welchen Gründen findet das Projekt „Post-Quanten-sichere Kommunikation für die Industrie 4.0“ im Handlungskonzept Quantentechnologien keine Erwähnung?

Das Handlungskonzept Quantentechnologien ist ein übergeordnetes Strategiedokument der Bundesregierung, welches auf andere Maßnahmen des Bundes mit deutlichem Bezug zu Quantentechnologien auf Programmebene und nicht auf der kleinteiligeren Projektebene referiert.

28. Hat die Bundesregierung Kenntnis von möglichen Auswirkungen quantentechnologischer Verfahren durch Drittstaaten auf die digitale Souveränität Deutschlands, und wenn ja, in welcher Weise will sie diese messen und ggf. darüber für die Öffentlichkeit Transparenz herstellen?

Wie in der Vorbemerkung der Bundesregierung dargestellt, sind die Cybersicherheit und damit auch die digitale Souveränität der Bundesrepublik Deutschlands potentiell zukünftig durch die Ausnutzung von Quantentechnologien gefährdet. Bzgl. der Transparenz in der Öffentlichkeit wird auf die Antwort zu Frage 6 verwiesen.

29. Hat die Bundesregierung davon Kenntnis, ob bei einer möglichen Überwachung des Bundesministeriums der Verteidigung durch US-amerikanische Geheimdienste (vgl. Vorbemerkung der Fragesteller) Quantentechnologie zum Einsatz kam, und wenn ja, in welcher Weise?

Es wird auf die Antworten zu den Fragen 7 und 8 verwiesen.

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.bundesanzeiger-verlag.de
ISSN 0722-8333