Nr. 1
Februar 2025

DGAP POLICY BRIEF

Wie Deutschland seine Position in der Post-Quanten-Kryptographie verbessern kann

Dr. Valentin Weber
Senior Research Fellow,
Zentrum für Geopolitik, Geoökonomie und Technologie

Maria Pericàs
Projektassistenz, Zentrum für Geopolitik, Geoökonomie und Technologie

In diesem DGAP Policy Brief werden die Auswirkungen des vor zwei Jahren begonnenen Übergangs zur Post-Quanten-Kryptographie (Post-Quantum Cryptography, PQC) untersucht. Zunächst wird bewertet, inwiefern die wichtigsten Technologieunternehmen in verschiedenen Sektoren quantensichere Verschlüsselung nutzen. Wir stellen fest, dass Firmen wie Amazon, IBM und Apple die Technologie bereits aktiv einsetzen, während dies bei keinem großen deutschen Unternehmen der Fall ist. Daher werden Empfehlungen formuliert, wie Deutschland diese Lücke am besten schließen kann.

- **Da die Bundeswehr und das BSI bei der quantensicheren Verschlüsselung Pionierarbeit leisten, sollten sie die deutsche Privatwirtschaft bei der Umsetzung unterstützen. Ohne eine praxisnahe Zusammenarbeit werden die Verteidigungsindustrie und die DAX-Unternehmen den Übergang nicht rechtzeitig schaffen.**

- **Die deutschen Bundesbehörden sollten den Privatsektor sensibilisieren. Chinas Angriffe gegen konventionelle Verschlüsselung werden immer fortschrittlicher. Sogenannte „Harvest-Now-Decrypt-Later"-Angriffe zielen darauf ab, Daten abzugreifen, um sie später zu entschlüsseln. Es ist höchste Zeit, sich um Quantensicherheit zu kümmern.**

- **Die von der Bundeswehr und anderen deutschen Bundesbehörden verwendete Messaging-Software ist noch nicht quantensicher. Diese Anwendungen sollten umgehend auf hybride Verschlüsselungsansätze umgestellt werden.**

- **Standardisierung hat den Übergang zur Quantenkryptographie signifikant beschleunigt. Daher sollten die deutsche Regierung und Unternehmen ihre Arbeit auf diesem Gebiet intensivieren, insbesondere in den Bereichen Cloud, Messaging, E-Mail und Fernzugriffssoftware.**

Am 1. Oktober 2024 hat Bundeskanzler Olaf Scholz die Ambitionen Deutschlands in Bezug auf Quantentechnologien dargelegt. „Unser Ziel ist klar: Wir wollen bei den Quantentechnologien weltweit führend sein", hieß es in seiner Rede.[1] Während Quantentechnologie die Bereiche Quantencomputer, -kommunikation, -sensorik und -verschlüsselung umfassen, konzentriert sich dieser DGAP Policy Brief nur auf einen Bereich – die Post-Quanten-Kryptographie bzw. Post-Quanten-Verschlüsselung. Mit Ausnahme eines Beispiels befasst er sich nicht mit der Quantenkommunikation, auch wenn diese eine weitere Möglichkeit zur Sicherung von Netzwerken darstellt.[2]

In Übereinstimmung mit Scholz' Aussage ist der *öffentliche* Sektor in Deutschland führend bei der Implementierung von Post-Quanten-Kryptographie in seinen Netzen. Die Bundeswehr zum Beispiel hat bahnbrechende Arbeit geleistet und Post-Quanten-Algorithmen zur Sicherung ihres 13.000 Kilometer langen Glasfasernetzes in ganz Deutschland eingesetzt.[3] Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist führend bei der Mitentwicklung von Standards für quantensichere Verschlüsselung.[4] Dies ist jedoch nicht genug.

Wenn Deutschland tatsächlich bei der Post-Quanten-Kryptographie führen will, müssen *private* Unternehmen ihre Anstrengungen verstärken. Derzeit verlieren sie international an Boden. Wie dieser Policy Brief zeigt, hinken die großen deutschen Technologieunternehmen bei der Post-Quanten-Kryptographie hinterher. Software AG, United Internet AG, BWI, TeamViewer und AnyDesk haben keine diesbezüglichen Pläne bekanntgegeben. Lediglich SAP hat begonnen, mit Post-Quanten-Kryptographie zu experimentieren, ist aber noch nicht über die Testphase hinausgekommen. Wie eine Studie von BSI und KPMG aus dem Jahr 2023 zeigt, stehen nicht primär in der IT-Branche tätige deutsche Unternehmen noch schlechter da.[5]

Es gibt wahrscheinlich noch keinen leistungsfähigen Quantencomputer, der herkömmliche Verschlüsselungsstandards brechen könnte; die Bedrohung scheint also in weiter Ferne zu liegen. Allerdings sammeln Länder bereits jetzt Daten, um sie später – voraussichtlich in den 2030er Jahren – mit entsprechend starken Quantencomputern zu entschlüsseln.[6] Angesichts der aktuellen technologischen Fortschritte in den USA, China und mehreren europäischen Ländern könnte ein Quantencomputer sogar noch deutlich früher dieses Ziel erreichen. Die chinesische Forschung zeigt sich besonders gut darin, konventionelle Verschlüsselung zu entziffern.[7] Folglich bleibt weniger Zeit für die Einführung der Post-Quanten-Kryptographie, als die Verantwortlichen in der Wirtschaft vielleicht denken.

Während einige Unternehmen noch zögern, haben andere konkrete Pläne zum Erreichen von Quantenresilienz entwickelt. Im Folgenden analysieren wir zunächst die aktuelle Phase des Übergangs zur Quantenkryptographie. Anschließend geben wir praktische Empfehlungen, wie Deutschland diesen Übergang nicht nur bewältigen, sondern auch den von seiner Regierung formulierten Führungsanspruch erfüllen kann.

1 „Wir profitieren von der weltweiten Zusammenarbeit': Scholz will Deutschland zum Zentrum der Quantentechnologie machen", Tagesspiegel, 01.10.2024: https://www.tagesspiegel.de/wirtschaft/wir-profitieren-von-der-weltweiten-zusammenarbeit-scholz-will-deutschland-zum-zentrum-der-quantentechnologie-machen-12467489.html (letzter Zugriff: Februar 2025)

2 Bei der Ausnahme handelt es sich um Cisco, ein Beispiel, auf das im Abschnitt über Cloud-Dienste verwiesen wird. Siehe auch Anmerkung 22.

3 „BWI modernisiert Weiterverkehrsnetz der Bundeswehr", Bundeswehr-Journal, 17.01.2024: https://www.bundeswehr-journal.de/2024/bwi-modernisiert-weitverkehrsnetz-der-bundeswehr (letzter Zugriff: Februar 2025).

4 „BSI-Projekt: Entwicklung einer sicheren Kryptobibliothek", BSI, kein Datum: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html (letzter Zugriff: Februar 2025).

5 „Gemeinsame Umfrage von BSI und KPMG in Deutschland zu 'Kryptografie und Quantencomputing'", BSI, 18.04.2023: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/BSI_KMPG_Quanten_230418.html (letzter Zugriff: Februar 2025).

6 „What is quantum-safe cryptography?", IBM, 04.09.2024, https://www.ibm.com/think/topics/quantum-safe-cryptography (letzter Zugriff: Februar 2025).

7 Natto Team, "The Red Dragon Searches for Pearls Through Quantum Tunneling – But You've Got the Wrong Paper," Natto Thoughts Substack, 22.10.2024: https://nattothoughts.substack.com/p/chinas-quantum-tunneling-breakthrough (letzter Zugriff: Februar 2025).

ZUSAMMENFASSUNG DER ERGEBNISSE

Wie in Tabelle 1 zusammengefasst, liefert der vorliegende Policy Brief einen Überblick über die Fortschritte in der Quantensicherheit von Unternehmen, die in Deutschland und/oder international in sieben Schlüsselsektoren einen beträchtlichen Marktanteil halten. Wir haben den aktuellen Stand in drei Hauptkategorien eingeteilt:

- **Quantensicher**: umfasst Produkte, die Post-Quanten-Algorithmen implementieren und/oder bestehende Protokolle mit Post-Quanten-Kryptographie aktualisiert haben. Diese Kategorisierung bedeutet keine vollständige Quantensicherheit; vielmehr umfasst sie Lösungen, die diesem Ziel vergleichsweise am nächsten kommen.

- **Testphase**: bezieht sich auf Produkte, die den Einsatz von Post-Quanten-Kryptographie-Algorithmen in ihren Diensten bereits erproben oder ankündigen, dass eine Einführung bevorsteht.

- **Quantenunsicher**: kennzeichnet Produkte, bei denen keine Arbeit an einer Implementierung von Post-Quanten-Kryptographie öffentlich bekannt ist.

Wie Tabelle 1 zeigt, wird Post-Quanten-Kryptographie vor allem in Browsern eingesetzt. Chrome, Brave und Edge verfügen bereits über Optionen zur Aktivierung hybrider Verschlüsselung, die klassische kryptographische Algorithmen mit Post-Quanten-Kryptographie kombiniert. Firefox und Tor Brow-ser befinden sich in der Testphase; nur Safari hat noch keine entsprechenden Schritte bekanntgegeben.

Ähnlich sieht es bei den Anbietern virtueller privater Netzwerke (VPNs) aus. ExpressVPN, MullvadVPN und NordVPN bieten Schutz vor Quanten-Computern; OpenVPN entwickelt momentan ebenfalls eine Lösung.

Cloud-Dienste sind etwa genauso weit. IBM Cloud und Amazon Web Services (AWS) vermarkten bereits fertige Lösungen; andere Anbieter wie SAP, Microsoft und Cisco arbeiten daran, Post-Quanten-Kryptographie in ihren Systemen einzusetzen.

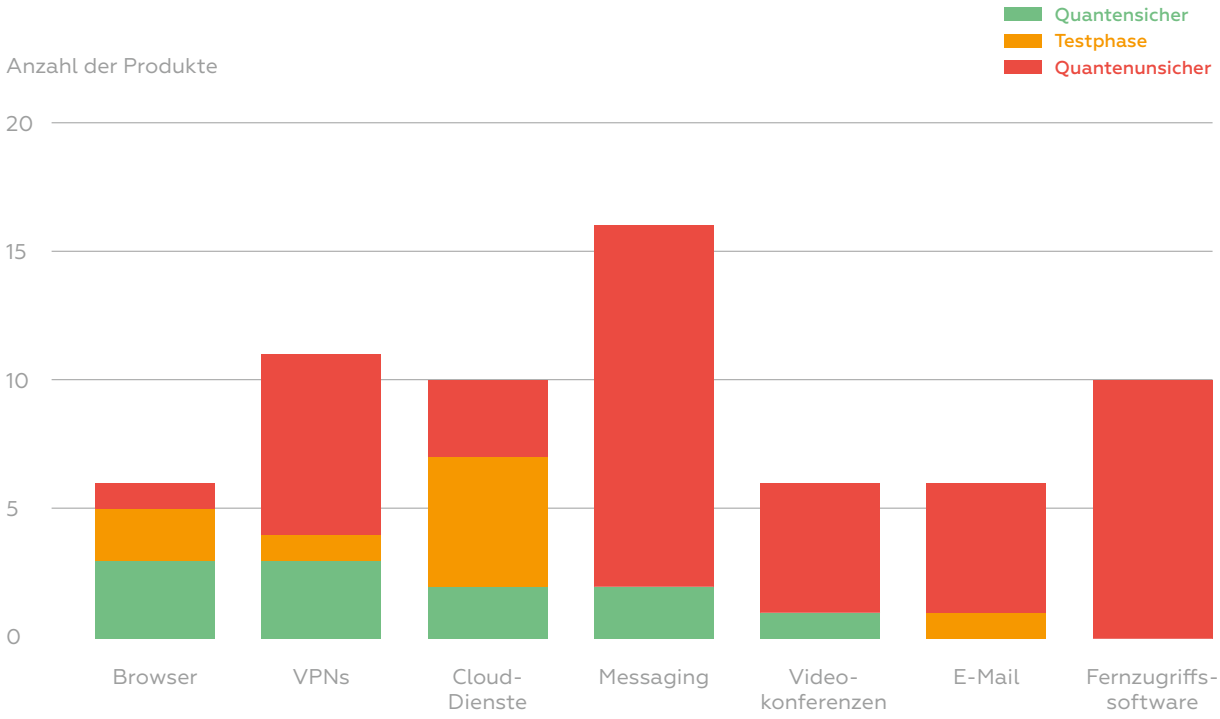
Bei den Messaging-Diensten stehen zwei Produkte zur Auswahl: Signal und iMessage. Beunruhigenderweise scheinen keine anderen Messaging-Dienste Post-Quanten-Kryptographie auch nur auszutesten, von vollumfänglicher Verwendung ganz zu schweigen.

Tabelle 1 – Quantenübergang in den Unternehmen der Schlüsselsektoren

	QUANTENSICHER	TESTPHASE	QUANTENUNSICHER
Browser	Brave Browser, Google Chrome, Microsoft Edge	Mozilla Firefox, Tor Browser	Safari
Cloud-Dienste	Amazon Web Services, IBM Cloud	Cisco Routers, Google Cloud, Linode, Microsoft, SAP	Oracle Cloud, Salesforce, Software AG
VPNs	ExpressVPN, MullvadVPN, NordVPN	OpenVPN	CyberGhost, IPVanish, PIA VPN, Private VPN, ProtonVPN, Surfshark, Windscribe
Messaging	iMessage, Signal		BundesMessenger, BwMessenger, Discord, Facebook Messenger, Google Messages, Kakao Talk, Line, Snapchat, Telegram, Threema, Viber, WhatsApp, Wire, Wire Bund
Video-konferenzen	Zoom Meetings		Facetime, Google Meet, Microsoft Teams, Skype, Webex
E-Mail		Proton Mail	AOL Mail, Gmail, GMX Mail, Outlook, Yahoo
Fernzugriffs-software			AnyDesk, Citrix Systems (Citrix Workspace), Dameware (SolarWinds), GoTo, Microsoft Remote Desktop Services, Parallels, Splashtop, TeamViewer, VNC Connect (RealVNC), Zoho (Assist)

Quelle: Eigene Zusammenstellung der Autoren

Chart 1 – Quantenübergang in den Schlüsselsektoren



Quelle: Eigene Zusammenstellung der Autoren

Bei Videokonferenzen gibt es nur einen quantensicheren Anbieter: Zoom. Microsoft Teams, Webex und andere große Anbieter haben es versäumt, Post-Quanten-Kryptographie einzusetzen.

Noch schlimmer ist die Lage in Sachen E-Mail und Fernzugriffssoftware. Kein einziger E-Mail-Anbieter hat bisher quantensichere Lösungen. Proton befindet sich als einziger Anbieter in der Testphase – zumindest wurde in einem Blogpost über Quantensicherheit gesprochen – eine einsatzbereite Lösung gibt es aber noch nicht. Am schlechtesten schneidet der Bereich Fernzugriffssoftware ab. Kein Unternehmen hat bisher auch nur angekündigt, Post-Quanten-Kryptographie zur Absicherung seiner Produkte auszutesten.

QUANTENBEREITSCHAFT NACH SEKTOR

Messaging

Quantensicher Unter den untersuchten Messaging-Apps setzen nur zwei bereits Post-Quanten-Algorithmen ein: **Signal** und **iMessage**.[8] Signal verwendet dazu sowohl traditionelle Kryptographie – das auf der elliptischen Kurve X25519 basierende Protokoll – als auch den Post-Quanten-Algorithmus CRYSTALS-Kyber.[9] Damit fügt Signal seiner bestehenden, für herkömmliche Computer schwer zu lösenden Verschlüsselungsschicht eine weitere hinzu, die gegen Quantencomputer effektiv ist. Dies kündigte Signal am 19. September 2023 an.

8 Signal, „Quantum Resistance and the Signal Protocol", Signal Blog, 19.09.2023: https://signal.org/blog/pqxdh/, https://security.apple.com/blog/imessage-pq3 (letzter Zugriff: Februar 2025).

9 Im Gegensatz zu Apple oder Zoom gibt Signal nicht an, welche Sicherheitsstufe der Post-Quanten-Kryptographie benutzt wird. Apple verwendet Kyber1024; Zoom verwendet Kyber768.

Am 21. Februar 2024 zog Apple nach und verkündete, einen ähnlichen hybriden Ansatz zu verfolgen und die herkömmliche Elliptische-Kurven-Kryptographie durch Quanten-Kryptographie (Kyber1024) zu ergänzen. Dabei ging Apple noch weiter als Signal und führte Post-Quanten-Rekeying ein: Hat ein Angreifer eine Konversation an einem bestimmten Punkt kompromittiert, macht es ihm diese Technologie unmöglich, weitere Nachrichten zu entziffern. Kurzum bietet Post-Quanten-Rekeying eine weitere Sicherheitsstufe.

Quantenunsicher Die Messenger, die wir untersucht haben, setzen keine Post-Quanten-Kryptographie ein. Dazu gehören **BwMessenger, BundesMessenger, Wire Bund, Google Messages, WhatsApp, Facebook Messenger, Telegram, Viber, Line, Discord, Kakao Talk, Snapchat, Threema** und **Wire**.

E-Mail

Testphase In einem Beitrag vom 24. Oktober 2023 erklärte **Proton**, mehrere Post-Quanten-Technologien ausgewählt zu haben: das digitale Signatur-Protokoll CRYSTALS-Dilithium, das die Identität des Absenders überprüft, sowie den Post-Quanten-Algorithmus CRYSTALS-Kyber.[10] Diese sollen in Kombination mit herkömmlicher Kryptographie (X25519) verwendet werden; noch ist das Unternehmen aber noch nicht soweit.

Quantenunsicher Alle anderen von uns untersuchten E-Mail-Anbieter **– Gmail, Outlook, Yahoo, AOL Mail** und **GMX Mail –** sind nicht quantensicher und werden es wahrscheinlich in der nahen Zukunft bleiben.

Videokonferenzen

Quantensicher Am 24. Mai 2024 kündigte Zoom an, dass von nun an **Zoom Meetings** durch Kyber768 geschützt werden können. Dabei bietet Kyber768 nur geringfügig weniger Sicherheit als das von Apple verwendete Kyber1024.[11] Wie andere Unternehmen verwendet auch Zoom einen hybriden Ansatz, der zum Schutz seiner Dienste traditionelle Kryptographie und Post-Quanten-Kryptographie kombiniert.[12] Allerdings ist Post-Quanten-Kryptographie bei Zoom Meetings optional; um diese zu aktivieren, muss erst die Ende-zu-Ende-Verschlüsselung manuell aktiviert werden.[13]

Quantenunsicher Außer Zoom gibt es keine Möglichkeit, quantensichere Videokonferenzen abzuhalten. **Skype, Webex, Microsoft Teams, Google Meet** und **Facetime** könnten durch einen Quantencomputer oder durch „Harvest-Now-Decrypt-Later"-Angriffe kompromittiert werden.

Fernzugriffssoftware

Quantenunsicher Fernzugriffssoftware ist am wenigsten auf Angriffe durch Quantencomputer vorbereitet. Keiner der großen Anbieter – z. B. **TeamViewer, GoTo, AnyDesk, Microsoft (Remote Desktop Services), Citrix Systems (Citrix Workspace), VNC Connect (RealVNC), Splashtop, Zoho Assist, Dameware (SolarWinds)** oder **Parallels** – hat auch nur die Absicht erklärt, Post-Quanten-Kryptographie einzuführen.

Browser

Quantensicher Seit August 2023 setzt **Google Chrome** nicht nur Elliptische-Kurven-Kryptografie (Algorithmus X25519) ein, sondern auch Kyber768, um im Netzwerkprotokoll TLS symmetrische Schlüssel zu erstellen.[14] Damit sind die Daten bei der Übertragung geschützt; die Erstellung der symmetrischen Schlüssel selbst ist aber anfällig für Angriffe. Daher ist Chrome auf quantenresistente Sitzungsschlüssel umgestiegen. Wenn Browser wie Chrome eine Verbindung zu einer Website herstellen oder ein Kennwort übertragen, wird die Verbindung mit TLS geschützt.

Da **Brave Browser** und **Microsoft Edge** auf Chromium, der Open-Source-Version von Chrome, basieren, verfügen sie auch über die von Chrome verwendete TLS-1.3-Funktion „hybridisierte Kyber-Unterstützung".

10 Proton, „Proton is building quantum-safe PGP encryption for everyone", Proton News, 24.10.2023: https://proton.me/blog/post-quantumencryption (letzter Zugriff: Februar 2025).

11 Peter Schwabe, „Cryptographic Suite for Algebraic Lattices (CRYSTALS)", PQ Crystals, 2017 veröffentlicht, am 23.12.2020 zuletzt aktualisiert: https://pq-crystals.org/kyber (letzter Zugriff: Februar 2025).

12 Zoom, „Your guide to post-quantum end-to-end encryption and how Zoom can help", Zoom Blog, am 24.05.2024 veröffentlicht, am 09.10.2024 zuletzt aktualisiert: https://www.zoom.com/en/blog/guide-to-post-quantum-end-to-end-encryption/ (letzter Zugriff: Februar 2025).

13 Zoom, „Using end-to-end encryption (E2EE) in Zoom meetings", Zoom Support, 15.07.2024: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (letzter Zugriff: Februar 2025).

14 Chromium, „Protecting Chrome Traffic with Hybrid Kyber KEM", Chromium Blog, 10.08.2023: https://blog.chromium.org/2023/08/protectingchrome-traffic-with-hybrid.html (letzter Zugriff: Februar 2025).

Testphase Im Januar 2024 erhielt die Entwicklerversion von **Firefox, „Firefox Nightly"**, ein Update, das die Unterstützung von Post-Quanten-Key-Agreement ermöglicht.[15] Es könnte bald in die Standardversion von Firefox übernommen werden.

Im März 2023 wurde angekündigt, dass der **Tor-Browser** zu quantensicheren Algorithmen übergehen würde.[16] Der erste Schritt sollte 2023 erfolgen: Größere Informationseinheiten sollen in kleinere Teile zerlegt werden. Diese Methode würde es ermöglichen, in Zukunft quantensichere Verschlüsselung zu implementieren.

Quantenunsicher Während iMessage von Apple ein Vorreiter der Post-Quanten-Kryptographie ist, hinkt das Unternehmen bei seinem **Safari-Browser** hinterher. Bis jetzt bleibt dieser angreifbar.

Cloud-Dienste

Quantensicher 2020 war **IBM Cloud** unter den ersten Anwendern von quantenresistenten Algorithmen, die eine sichere Kommunikation zwischen Clients und Servern ermöglichen. Wie so oft wird hier ein hybrider Ansatz verwendet; für quantensicheren Schlüsselaustausch sorgen Kyber512, Kyber768 und Kyber1024.[17]

Im Juni 2023 gab **Amazon Web Services** (AWS) an, dass eine Reihe seiner Dienste – darunter AWS Key Management Service, AWS Certificate Manager und AWS Secrets Manager – bereits einen Post-Quanten-Hybrid-Schlüsselaustausch (Kyber) einsetzen.[18]

Testphase **SAP** hat einige Proofs of Concept für die Durchführbarkeit der Einführung quantenresistenter Algorithmen entwickelt; noch wurden aber keine solchen Algorithmen eingesetzt.[19] Im September 2024 verkündete **Microsoft**, es habe die Unterstützung für Post-Quanten-Algorithmen in seiner kryptografischen Bibliothek SymCrypt veröffentlicht.[20]

Cisco hat ein Secure Key Integration Protocol (SKIP) entwickelt, mit dem Cisco-Geräte von Quantenschlüsselverteilungssystemen (QKD) bereitgestellte quantensichere Schlüssel verwenden können.[21]

Linode von Akamai Technology hat Open-Source-Implementierungen von Post-Quanten-Algorithmen getestet, setzt sie aber bisher nicht großflächig ein.[22]

Google Cloud verwendet anders als die meisten Unternehmen nicht Kyber, sondern den NTRU-HRSS-KEM-Algorithmus, da der Status von Kyber als geistiges Eigentum noch unklar ist.[23] Der Algorithmus wird jedoch nur für die interne Kommunikation verwendet, nicht für die Google-Cloud-Kundschaft.

Quantenunsicher Die deutsche **Software AG** sowie die US-amerikanischen Unternehmen **Salesforce** und **Oracle Cloud** haben nicht angekündigt, Post-Quanten-Kryptographie testen zu wollen, sind also weit davon entfernt, diese einzusetzen.

Virtuelle private Netzwerke (VPNs)

Quantensicher Am 25. Oktober 2023 verkündete **ExpressVPN**, sein Lightway-VPN-Protokoll um eine quantensichere Lösung erweitert zu haben.[24] Es verwendet nun P256_KYBER_LEVEL1 für UDP und P521_KYBER_LEVEL5 für TCP. Sowohl UDP als auch

15 Cloudflare, „The state of the post-quantum Internet", The Cloudflare Blog, 05.03.2024: https://blog.cloudflare.com/pq-2024/ (letzter Zugriff: Februar 2025).

16 Tor, „Post Quantum Cryptography", Tor Project, 02.2023: https://forum.torproject.org/t/post-quantum-cryptography/6563/2 (letzter Zugriff: Februar 2025).

17 IBM, „Introducing Quantum-Safe Crypto TLS for IBM Key Protect", IBM Blog, 03.12.2020: https://www.ibm.com/blog/introducing-quantum-safecrypto-tls-for-ibm-key-protect/ (letzter Zugriff: Februar 2025).

18 Amazon Web Services, „Post-quantum hybrid SFTP file transfers using AWS Transfer Family", AWS Security Blog, 13.06.2023: https://aws.amazon.com/blogs/security/post-quantum-hybrid-sftp-file-transfers-using-aws-transfer-family (letzter Zugriff: Februar 2025).

19 SAP, „SAP and Quantum Technologies", SAP News Center, 19.11.2021: https://news.sap.com/2021/11/sap-and-quantum-technologies/ (letzter Zugriff: Februar 2025).

20 Microsoft, „Microsoft's quantum-resistant cryptography is here", Microsoft Tech Community, 09.09.2024: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780 (letzter Zugriff: Februar 2025).

21 Cisco setzt auf Quantenkommunikation setzt und erweitert seine Kommunikationsnetzwerke um Post-Quanten-Kryptographie. Cisco, „Bringing post-quantum cryptography to communications networks", Cisco UK & Ireland Blog, 10.11.2023: https://gblogs.cisco.com/uki/bringing-post-quantum-cryptography-to-communications-networks/ (letzter Zugriff: Februar 2025).

22 Akamai, „Akamai and the Adoption of Post-Quantum Cryptography", Akamai Blog, 27.04.2023: https://www.akamai.com/blog/security/akamai-andpost-quantum-cryptography (letzter Zugriff: Februar 2025).

23 Google Cloud, „Securing tomorrow today: Why Google now protects its internal communications from quantum threats", Google Cloud Blog, 19.11.2022: https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms?hl=en (letzter Zugriff: Februar 2025).

24 ExpressVPN, „ExpressVPN launches post-quantum protection on Lightway", EpxressVPN News, 25.10.2023: https://www.expressvpn.com/blog/expressvpn-launches-post-quantum-protection-on-lightway/ (letzter Zugriff: Februar 2025).

TCP sind Datenübertragungsprotokolle – Regeln, die festlegen, wie Daten zwischen Geräten übertragen werden.

MullvadVPN gab im August 2024 bekannt, auf seinen WireGuard-Servern quantensichere Classic-McEliece- und Kyber-Algorithmen zu verwenden.[25]

Ende September 2024 brachte **NordVPN** im Rahmen eines Linux-App-Updates das erste Post-Quanten-Kryptographie-Upgrade für das Nordlynx-Protokoll auf den Markt. Das Unternehmen plant, diese Funktionalität auf alle seine Anwendungen auszuweiten.[26]

Testphase Um 2020 veröffentlichte Microsoft eine Version von **OpenVPN**, die Post-Quanten-Kryptographie in die VPN-Software integriert: Post-Quantum Crypto VPN.[27]

Quantenunsicher Während einige wenige Unternehmen Post-Quanten-Kryptographie in ihren Netzen einsetzen, sind die meisten in diesem Bereich untätig geblieben. Dazu gehören: **Surfshark, PIA VPN, Private VPN, CyberGhost, Windscribe, IPVanish** und **ProtonVPN.**

UMFANG DER UNTERSUCHUNG

Unsere Untersuchung basiert auf einer umfassenden Prüfung öffentlich zugänglicher Informationen, einschließlich offizieller Dokumente, Pressemitteilungen und öffentlicher Erklärungen ausgewählter Unternehmen. Sie stützt sich ausschließlich auf Open-Source-Daten; eventuelle unveröffentlichte Implementierungen der Post-Quanten-Kryptographie wurden bei den Ergebnissen also nicht berücksichtigt. Trotz der möglichst umfassenden Recherche können wir nicht ausschließen, dass Aktualisierungen übersehen oder erst nach Oktober 2024 veröffentlicht wurden, als wir unsere Datenzusammenstellung abgeschlossen hatten.

Wir haben die wichtigsten Unternehmen aus den Schlüsselindustrien der Informations- und Kommunikationstechnologie einbezogen und dabei auch auf geografische Vielfalt geachtet. Chinesische Plattformanbieter – ob vor oder nach der Quantenwende – haben wir jedoch nicht einbezogen, da davon auszugehen ist, dass diese Plattformen auf jeden Fall durch staatliche Anforderungen zur Datensammlung unsicher sind.[28] Jede Form der Verschlüsselung wird von China geschwächt und unterwandert. Es ist möglich, dass wir weitere wichtige Plattformen übersehen haben; sollte dies der Fall sein, geschah dies unbeabsichtigt.

25 AlternativeTo, „Mullvad introduces quantum-resistant VPN tunnels for enhanced future-proof security", 30.08.2024: https://alternativeto.net/news/2024/8/mullvad-introduces-quantum-resistant-vpn-tunnels-for-enhanced-future-proof-security; Mullvad VPN, "Stable Quantum-resistant tunnels in the app!", Mullvad Blog, 06.04.2023: https://mullvad.net/en/blog/stable-quantum-resistant-tunnels-in-the-app (letzter Zugriff, beide Quellen: Februar 2025).

26 NordVPN, „NordVPN launches first app with post-quantum encryption support", NordVPN Blog, 30.09.2024: https://nordvpn.com/blog/nordvpn-linux-post-quantum-encryption-support (letzter Zugriff: Februar 2025).

27 Microsoft, „Post-quantum Cryptography", Microsoft Research, kein Datum: https://www.microsoft.com/en-us/research/project/post-quantum-cryptography (letzter Zugriff: Februar 2025).

28 Jeffrey Knockel et al., „Privacy and Security Issues in BAT Web Browsers", 6th USENIX Workshop on Free and Open Communications on the Internet, 08.08.2016: https://www.usenix.org/conference/foci16/workshop-program/presentation/knockel; Valentin Weber, „How China's Control of Information is a Cyber Weakness", Lawfare, 12.11.2020: https://www.lawfaremedia.org/article/how-chinas-control-information-cyber-weakness (letzter Zugriff, beide Quellen: Februar 2025).

POLICY-EMPFEHLUNGEN FÜR DEUTSCHLAND

Die obige Analyse legt dar, wo Deutschland derzeit beim Übergang zu einer quantenresistenten – also auf Post-Quanten-Kryptographie basierten – Infrastruktur steht. Während der staatliche Sektor in Deutschland einige Fortschritte zeigt, ist der private deutlich anfälliger. Auf der anderen Seite des Atlantiks sieht es anders aus: In den Vereinigten Staaten haben einige Unternehmen ihre Bemühungen um Quantensicherheit bemerkenswert beschleunigt. Doch auch dort hinken viele noch hinterher und bleiben anfällig für „Harvest-Now-Decrypt-Later"-Angriffe, bei denen Daten für die spätere Entschlüsselung gesammelt werden. Um international aufzuholen, sollten deutsche Akteure die folgenden Schritte unternehmen:

- **Standardisierung intensivieren –** Standardisierung scheint der wichtigste Faktor für den Übergang zur Quantenkryptographie zu sein. Die meisten solchen Übergänge erfolgten nach der Auswahl und Bekanntgabe von vier quantenresistenten Verschlüsselungsalgorithmen durch das US-amerikanische National Institute of Standards and Technology (NIST) im Juli 2022. Die Bemühungen des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) und des E-Mail-Dienstleisters Proton, OpenPGP-Standards um ein asymmetrisches Post-Quanten-Kryptographiesystem zu erweitern, sind in diesem Zusammenhang zu begrüßen und zu unterstützen.

- **Just do it –** Signal und iMessage haben gezeigt, dass die Aktualisierung von Messaging-Protokollen möglich ist. Deutsche Produkte müssen ihrem Beispiel folgen und den Übergang vollziehen. Weder BWMessenger noch BundesMessenger sind derzeit quantensicher – und dafür gibt es einfach keinen guten Grund.

- **Make it easy –** Deutsche Unternehmen müssen quantensichere Dienste bei der Einführung möglichst nutzerfreundlich gestalten. Gegenbeispiele sind MullvadVPN sowie die Browser Chrome, Brave und Edge: Hier sind quantensichere Funktionen optional und müssen aktiv eingestellt werden. Darüber hinaus entsteht mitunter der falsche Eindruck, die Aktivierung dieser Funktionen würde die Sicherheit mindern anstatt umgekehrt. So warnt Chrome bei der Umschaltung auf Post-Quanten-Kryptografie: „Sie könnten … Ihre Sicherheit oder Ihre Privatsphäre gefährden."[29] Das motiviert nicht gerade zur Nutzung der Funktion. Im Fall von Zoom erfordert quantensichere Kommunikation die Aktivierung von Ende-zu-Ende-Verschlüsselung; man muss sich also für alles oder nichts entscheiden. Es wäre zielführender, Zoom-Anrufe standardmäßig Ende zu Ende inkl. Post-Quanten-Kryptographie zu verschlüsseln.

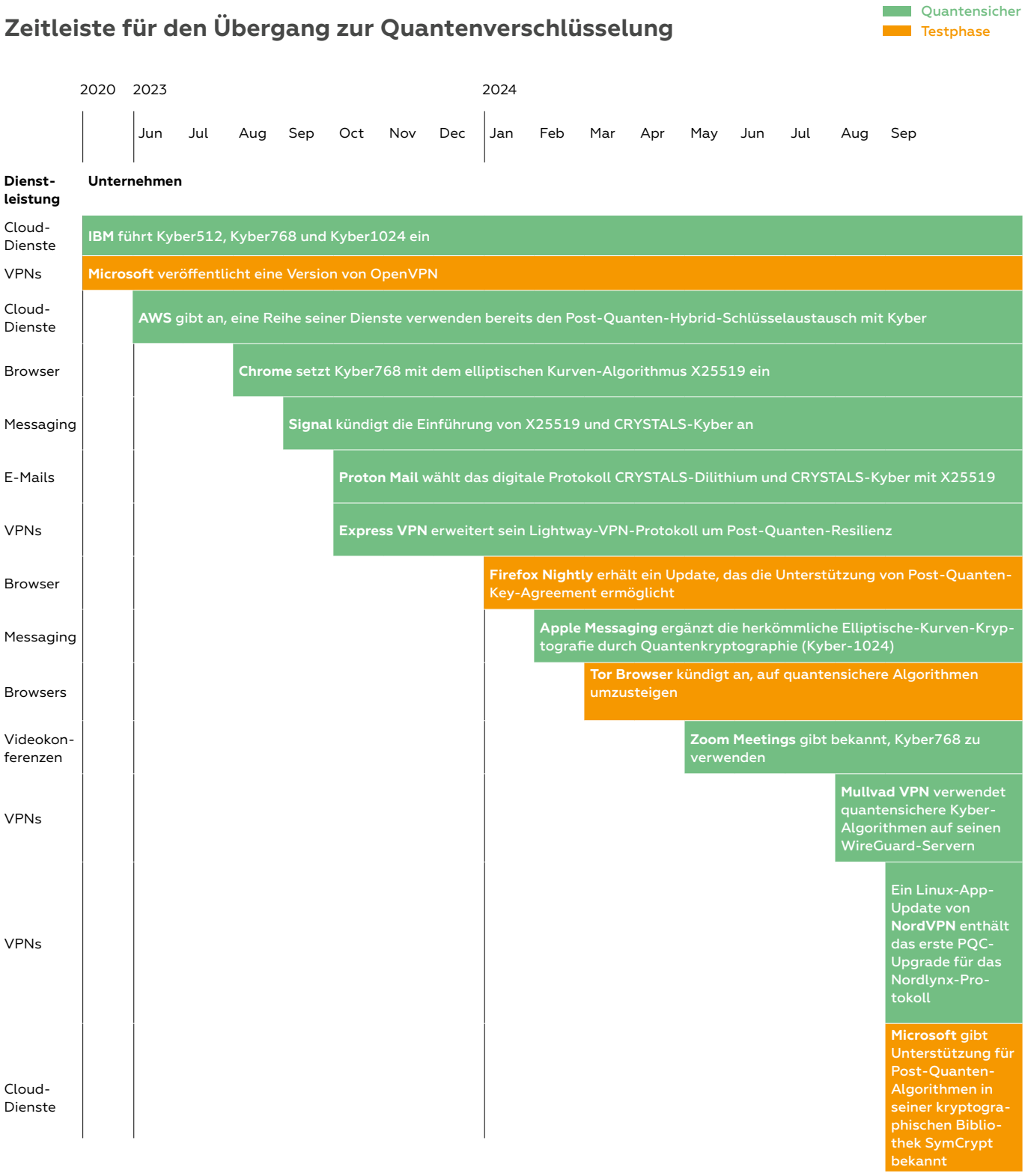
- **Mehr Transparenz –** Unternehmen müssen deutlich machen, wo sie beim Quantenphasenübergang stehen. SAP zum Beispiel meldet, Proofs of Concept entwickelt zu haben, stellt aber keinen Zeitplan für den Einsatz quantensicherer Lösungen bereit. Andere geben an, dass nur Teile ihrer Produkte quantensicher sind. Das Quanten-Update von NordVPN gilt nur für die Linux-App; das von MullvadVPN nur für die Desktop-App und nicht für iOS oder Android. Eine genauere Erklärung, warum diese Entscheidungen getroffen wurden, wäre hilfreich.

Maria Pericàs Riera und Valentin Weber danken Heike Hagemeier für ihr aufschlussreiches Feedback zu früheren Entwürfen dieses DGAP Policy Briefs. Sollte sich dennoch eine Ungenauigkeit eingeschlichen haben, liegt dies in der alleinigen Verantwortung des Autors und der Autorin.

29 Google Chrome Administrative Templates (Computers): https://admx.help/?Category=Chrome&Policy=Google.Policies.Chrome::EnableExperimentalPolicies (letzter Zugriff: Februar 2025).

ANHANG

Zeitleiste für den Übergang zur Quantenverschlüsselung



Quelle: Eigene Zusammenstellung der Autoren

Chart 2 – Hauptsitzstandorte ausgewählter Unternehmen

HAUPTSITZ LAND	HAUPTSITZ STADT	UNTERNEHMEN	PRODUKT
Britische Jungferninseln	British Virgin Islands	Kape Technologies	ExpressVPN
Kanada	Toronto, Ontario	Windscribe	Windscribe
Deutschland	Stuttgart, Baden-Württemberg	AnyDesk	AnyDesk
	Meckenheim, North Rhine-Westphalia	BWI	BwMessenger
	Meckenheim, North Rhine-Westphalia	BWI	BundesMessenger
	Walldorf, Baden-Württemberg	SAP	SAP
	Darmstadt, Hesse	Software AG	Software AG
	Goeppingen, Baden-Württemberg	TeamViewer	TeamViewer
	Karlsruhe, Baden-Württemberg	United Internet AG	GMX Mail
Indien	Chennai, Tamil Nadu	Zoho	Zoho Assist
Japan	Tokyo	Line	Line
Luxemburg	Luxembourg	Skype – Microsoft-owned	Skype
	Luxembourg	Viber	Viber
Panama	Panama City	NordVPN	NordVPN
Rumänien	Bucharest	CyberGhost	CyberGhost
Südkorea	Jeju City	Kakao Corporation	Kakao Talk
Schweden	Gothenburg	MullvadVPN	MulllvadVPN
	Sollentuna	Private VPN	Private VPN
Schweiz	Geneva	Proton	Proton VPN
	Geneva	Proton	Proton Mail
	Pfäffikon	Threema	Threema
	Zug	Wire Swiss	Wire Bund
	Zug	Wire Swiss	Wire

HAUPTSITZ LAND	HAUPTSITZ STADT	UNTERNEHMEN	PRODUKT
Niederlande	Amsterdam	Surfshark	Surfshark
Vereinigte Arabische Emirate	Dubai	Telegram	Telegram
Vereinigtes Königreich	Cambridge	RealVNC	VNC Connect
Vereinigte Staaten	Philadelphia, PA	Akamai Technologies	Linode
	Mountain View, CA	Alphabet	Google Chrome
	Mountain View, CA		Google Cloud
	Mountain View, CA		Google Messages
	Mountain View, CA		Google Meet
	Mountain View, CA		Gmail
	Seattle, WA	Amazon	Amazon Web Services
	New York, NY	AOL	AOL Mail
	Cupertino, CA	Apple	Safari
	Cupertino, CA		iMessage
	Cupertino, CA		Facetime
	San Francisco, CA	Brave	Brave Browser
	San Jose, CA	Cisco	Cisco Routers
	San Jose, CA		Webex
	Fort Lauderdale, FL	Citrix Systems	Citrix Workspace
	Austin, TX	Dameware	SolarWinds
	San Francisco, CA	Discord	Discord
	Boston, MA	GoTo	GoTo
	Armonk, NY	IBM	IBM Cloud
	Menlo Park, CA	Meta	WhatsApp
	Menlo Park, CA		Facebook Messenger
	Redmond, WA	Microsoft	Microsoft Edge
	Redmond, WA		Microsoft Teams
	Redmond, WA		Outlook
	Redmond, WA		Microsoft Remote Desktop Services
	San Francisco, CA	Mozilla Foundation	Mozilla Firefox
	Pleasanton, CA	OpenVPN	OpenVPN
	Austin, TX	Oracle	Oracle Cloud
	Seattle, WA	Parallels	Parallels
	Denver, CO	PIA VPN	PIA VPN
	San Francisco, CA	Salesforce	Salesforce
	Mountain View, CA	Signal	Signal
	Santa Monica, CA	Snap	Snapchat
	Cupertino, CA	Splashtop	Splashtop
	Winchester, NH	The Tor Project	Tor Browser
	New York, NY	Yahoo	Yahoo
	New York, NY	Ziff Davis	IPVanish
	San Jose, CA	Zoom Video Communications	Zoom Meetings

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Übersetzung Alexandra Berlina/
Pavel Sirotkin (dolmetscher.team)

Layout Daniel Faller

Design Konzept WeDo