No. 25
November 2024

DGAP POLICY BRIEF

How Germany Can Improve Its Standing in Post-Quantum Cryptography

Dr. Valentin Weber
Senior Research Fellow,
Center for Geopolitics,
Geoeconomics, and Technology

Maria Pericàs
Project Assistant, Center for
Geopolitics, Geoeconomics,
and Technology

This DGAP Policy Brief examines the impact of the major shift to post-quantum cryptography that occurred two years ago. First, it assesses how extensively major technology companies in various sectors are deploying quantum-proof encryption. Then – given that companies such as Amazon, IBM, and Apple are already actively deploying it while no major German company yet has – it offers Germany recommendations on how it can best close this gap.

- As the Bundeswehr and the BSI do pioneering work in quantum-secure encryption, they should support the German private sector in implementing it. Without practical cooperation, the defense industry and DAX companies will fail to transition in time.
- German federal agencies should raise awareness in the private sector. Recent Chinese advances in challenging conventional encryption – as well as "harvest now, decrypt later" attacks – mean that now is the time to become quantum-resilient.
- The messaging software used by the Bundeswehr and other German federal entities is not yet quantum resilient. These software applications should be transitioned to hybrid encryption approaches immediately.
- As standardization has been key to propelling the quantum transition, Germany's government and companies should double-down on it, especially in the cloud, messaging, email, and remote access software sectors.

On October 1, 2024, Chancellor Olaf Scholz set out Germany's ambition in quantum technologies. "Our goal is clear: to be global leader in quantum technologies," he stated.[1] While quantum technologies encompass quantum computing, communication, sensing, and encryption, this DGAP Policy Brief focuses on only one of these three branches – post-quantum cryptography, also known as post-quantum encryption. With the exception of one example, it does not deal with quantum communication, which is another way of securing networks.[2]

In line with Scholz's statement, Germany's *public* sector is leading in the implementation of post-quantum cryptography in their networks. The Bundeswehr, for instance, has done groundbreaking work by deploying quantum encryption algorithms to secure its 13,000-kilometer fiber network across Germany.[3] Similarly, Germany's Federal Office for Information Security (BSI) has been a leader in co-developing standards for quantum-secure encryption.[4] However, this is not enough.

If Germany wants to be a leader in quantum encryption, its *private* companies will have to step up their efforts. Currently, they are losing ground internationally. As this policy brief shows, Germany's larger technology companies are behind in implementation – at least when it comes to post-quantum encryption. Software AG, United Internet AG, BWI, TeamViewer, and AnyDesk are far from having a public plan on deploying this technology. Only SAP has started to experiment with post-quantum encryption but has not gone beyond trials. As a 2023 study by the BSI and KPMG shows, German companies that are not primarily in the IT sector fare even worse.[5]

SCOPE OF OUR RESEARCH

Our research is based on an extensive review of publicly available information, including official documents, press releases, and public statements from selected companies. It relies exclusively on open-source data, meaning that any unpublished/undisclosed implementation of quantum cryptography is not reflected in our findings. While the research we conducted was as comprehensive as possible, we cannot rule out that some updates may have been overlooked or released after October 2024 when we completed our data compilation.

We included the major companies in key information and communication technology industries, while also aiming to provide for geographic diversity. We did not, however, include Chinese platform providers – whether in the context of the pre- or post-quantum-encryption age – because it is assumed that the data collection requirements of the Chinese state make these insecure from the outset.[6] Any form of encryption is weakened and subverted by China. Yet, it is possible that we inadvertently omitted other major platforms. Any omissions of major players in the industries mentioned were not intended.

1 Madeline Chambers, "Germany aims to be world leader in quantum technologies, says Scholz," *Reuters*, October 1, 2024: https://www.reuters.com/technology/germany-aims-be-world-leader-quantum-technologies-says-scholz-2024-10-01/#:~:text=%22Our%20goal%20is%20clear%3A%20to,on%20quantum%20technology%20since%202020 (accessed October 18, 2024).

2 The exception is the Cisco example referred to in the section on cloud services below. See also note 22.

3 "BWI modernisiert Weiterverkehrsnetz der Bundeswehr" [BWI modernizes the Bundeswehr's onward transpot network], *Bundeswehr-Journal*, January 17, 2024: https://www.bundeswehr-journal.de/2024/bwi-modernisiert-weitverkehrsnetz-der-bundeswehr/ (accessed November 7, 2024).

4 "BSI-Projekt: Entwicklung einer sicheren Kryptobibliothek" [BSI project: Development of a secure crypto library], BSI, no date: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html (accessed November 8, 2024).

5 "Gemeinsame Umfrage von BSI und KPMG in Deutschland zu 'Kryptografie und Quantencomputing'" ["Joint survey by BSI and KPMG in Germany on 'Cryptography and quantum computing'"], BSI, April 18, 2023: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/BSI_KMPG_Quanten_230418.html (accessed November 8, 2024).

6 Jeffrey Knockel et al., "Privacy and Security Issues in BAT Web Browsers," 6th USENIX Workshop on Free and Open Communications on the Internet, August 8, 2016: https://www.usenix.org/conference/foci16/workshop-program/presentation/knockel; Valentin Weber, "How China's Control of Information is a Cyber Weakness," *Lawfare*, November 12, 2020: https://www.lawfaremedia.org/article/how-chinas-control-information-cyber-weakness (both accessed October 18, 2024).

As it is likely that the first powerful quantum computer that could break traditional encryption standards does not yet exist, the threat appears far away. However, countries are already harvesting data now that they will decrypt later when quantum computers will be powerful enough to break encryption, probably in the 2030s.[7] Yet, with current breakneck advances in technology among the United States, China, and countries in Europe, an encryption-breaking quantum computer could arrive sooner rather than later. Chinese researchers have been shown to be particularly advanced in developing approaches to breaking asymmetric encryption.[8] As a result, there is less time to deploy post-quantum cryptography than business leaders may think.

While some companies remain sluggish, others have already drawn up serious plans on how to accomplish the transition to quantum resilience. Below, we first analyze the quantum transition that is, at least partially, already underway. Then, we provide practical recommendations on how Germany can not only navigate this transition but also fulfill the ambition to leadership set out by its government.

SUMMARY OF FINDINGS

As summarized in Table 1, this paper provides an overview of the steps toward quantum resilience taken by major companies that hold a considerable market share in Germany and/or internationally in seven key sectors. We have grouped the companies' progress into three main categories:

- **Quantum Secure**: encompasses products that have implemented post-quantum algorithms and/or updated existing protocols with quantum-secure cryptography. This categorization does not mean that these products are entirely quantum secure, but rather that they are closest to achieving this goal as compared to other products.
- **Quantum Experimental**: refers to companies that have already tested the deployment of quantum-secure encryption algorithms in their services or indicated that implementation is forthcoming.
- **Quantum Insecure**: indicates companies that have not publicly disclosed any efforts toward implementing quantum-secure encryption.

Table 1 – Quantum Transition Across Companies in Key Sectors

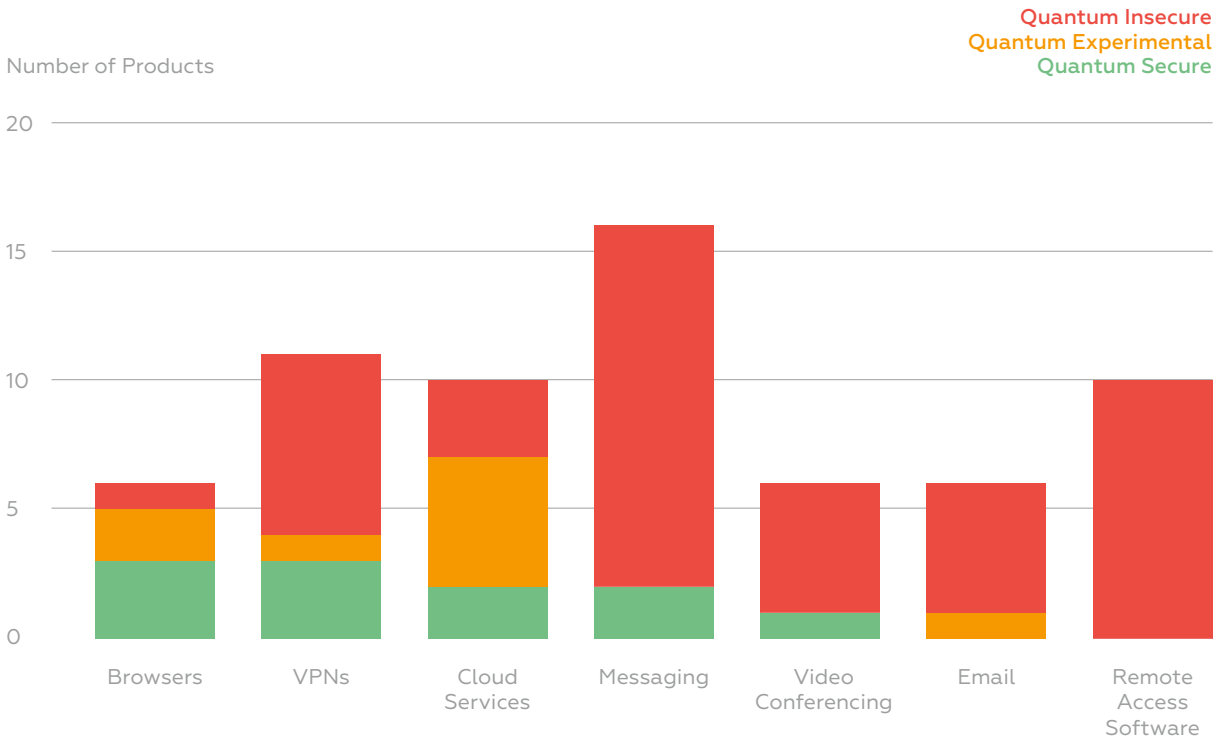
	QUANTUM SECURE	QUANTUM EXPERIMENTAL	QUANTUM INSECURE
Browsers	Brave Browser, Google Chrome, Microsoft Edge	Mozilla Firefox, Tor Browser	Safari
Cloud Services	Amazon Web Services, IBM Cloud	Cisco Routers, Google Cloud, Linode, Microsoft, SAP	Oracle Cloud, Salesforce, Software AG
VPNs	ExpressVPN, MullvadVPN, 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 Conferencing	Zoom Meetings		Facetime, Google Meet, Microsoft Teams, Skype, Webex
Email		Proton Mail	AOL Mail, Gmail, GMX Mail, Outlook, Yahoo
Remote Access Software			AnyDesk, Citrix Systems (Citrix Workspace), Dameware (SolarWinds), GoTo, Microsoft Remote Desktop Services, Parallels, Splashtop, TeamViewer, VNC Connect (RealVNC), Zoho (Assist)

Source: Authors' own compilation

7 "What is quantum-safe cryptography?", IBM, September 4, 2024: https://www.ibm.com/topics/quantum-safe-cryptography (accessed October 18, 2024).

8 Natto Team, "The Red Dragon Searches for Pearls Through Quantum Tunneling – But You've Got the Wrong Paper," Natto Thoughts Substack, October 22, 2024: https://nattothoughts.substack.com/p/chinas-quantum-tunneling-breakthrough (accessed October 25, 2024).

Chart 1 – Quantum Transition Across Key Sectors



Source: Authors' own compilation

As illustrated in Chart 1, the leading industry in deploying quantum-safe encryption is browsers. Chrome, Brave, and Edge already have options to enable hybrid encryption, combining classical cryptographic algorithms with post-quantum cryptography algorithms. Firefox and Tor Browser are in the experimental stage, while Safari has not yet announced any advances in this regard.

Just as advanced are cloud services. IBM Cloud and Amazon Web Services (AWS) both have commercialized solutions, and many other providers – such as SAP, Microsoft, and Cisco – are actively working to deploy quantum-resilient encryption in their systems.

Providers of virtual private networks (VPNs) fare similarly. ExpressVPN, MullvadVPN, and NordVPN offer customers the ability for their traffic to become safe from quantum snooping and OpenVPN is being developed in this direction.

Regarding messaging services, there is a choice of two major messengers to choose from: Signal and iMessage. However, worryingly, no other messaging services appear to be deploying post-quantum encryption methods, let alone experimenting with them.

Video conferencing is already leaning to the other side of the spectrum. If users want a quantum-proof experience, they can only rely on Zoom as the market does not offer any alternatives. Microsoft Teams, Webex, and other major providers have failed to deploy quantum-proof encryption.

It is even worse when it comes to email or remote access software. Not a single email provider has yet to offer quantum-proof solutions. While Proton is the only email service provider that has explicitly discussed quantum resilience in a blogpost, it does not yet have any solutions. The remote access software industry is the worst performer. No company has even announced yet that it is experimenting with quantum encryption to secure their products, let alone deploying them.

PREPAREDNESS IN INDIVIDUAL SECTORS

Messaging

Quantum Secure: Of the messaging apps we examined, only two have already deployed post-quantum algorithms: **Signal** and **iMessage**.[9] To accomplish this, Signal uses both the elliptic curve key agreement protocol X25519 (traditional cryptography) as well as the post-quantum cryptographic algorithm CRYSTALS-Kyber.[10] This means that, in addition to its already existing layer of encryption that contains problems that are difficult for traditional computers to solve, Signal added a layer of encryption with problems that are very difficult for quantum computers to solve. Signal announced this deployment on September 19, 2023.

On February 21, 2024, Apple followed suit by proclaiming that it is taking a similar hybrid approach that adds quantum cryptography (Kyber1024) on top of traditional elliptic curve cryptography. Yet, Apple went even further than Signal by introducing post-quantum rekeying. This technology ensures that, even if an attacker managed to compromise a conversation at a certain point, the attacker would lose the ability to do so for new messages. In short, post-quantum rekeying offers yet another layer of security.

Quantum Insecure: Meanwhile, most – if not all – other messengers we examined do not deploy post-quantum cryptography. Those are **BwMessenger, BundesMessenger, Wire Bund, WhatsApp, Facebook Messenger, Google Messages, Telegram, Viber, Line, Discord, Kakao Talk, Snapchat, Threema,** and **Wire**.

Email

Quantum Experimental: In a post on October 24, 2023, **Proton** stated that it had selected the CRYSTALS-Dilithium digital protocol for digital signatures, which verifies the sender's identity, and CRYSTALS-Kyber, a post-quantum cryptography algorithm, for use in its encryption in combination with X25519 (traditional cryptography).[11] However, these security features have yet to be deployed.

Quantum Insecure: All of the other email service providers that we looked at – **Gmail, Outlook, Yahoo, AOL Mail,** and **GMX Mail** – are unprepared and will likely remain so in the near future.

Video Conferencing

Quantum Secure: On May 24, 2024, Zoom announced that, from then on, **Zoom Meetings** would also be protected by Kyber768, which provides a bit less security than the Kyber1024 used by Apple.[12] Like other companies, Zoom uses a hybrid approach that combines traditional and post-quantum cryptography to protect its services.[13] Yet, Zoom Meetings does not use post-quantum cryptography by default. Users need to manually enable end-to-end-encryption to also use the quantum-proof algorithm.[14]

Quantum Insecure: Worryingly for users, Zoom offers the only choice to have post-quantum resilient video conferencing. **Skype, Webex, Microsoft Teams, Facetime,** and **Google Meet** are all open to being compromised by a quantum computer or "harvest now, decrypt later" attacks.

Remote Access Software

Quantum Insecure: Remote access software is the sector that is the least prepared for quantum computer attacks. None of the major providers, e.g., **TeamViewer, GoTo, AnyDesk, Microsoft (Remote Desktop Services), Citrix Systems (Citrix Workspace), VNC Connect (RealVNC), Splashtop, Zoho Assist, Dameware (SolarWinds),** or **Parallels,** have declared that they are working on deploying post-quantum cryptography to protect their services.

9 Signal, "Quantum Resistance and the Signal Protocol," *Signal Blog*, September 19, 2023: https://signal.org/blog/pqxdh/, https://security.apple.com/blog/imessage-pq3/ (accessed October 18, 2024).

10 Unlike Apple or Zoom, Signal does not specify what security level of post-quantum cryptography it is using. Apple uses Kyber1024; Zoom uses Kyber768.

11 Proton, "Proton is building quantum-safe PGP encryption for everyone," *Proton News*, October 24, 2023: https://proton.me/blog/post-quantum-encryption (accessed October 18, 2024).

12 Peter Schwabe, "Cryptographic Suite for Algebraic Lattices (CRYSTALS)," *PQ Crystals*, designed in 2017 and last updated on December 23, 2020: https://pq-crystals.org/kyber/ (accessed October 18, 2024).

13 Zoom, "Your guide to post-quantum end-to-end encryption and how Zoom can help," *Zoom Blog* (published on May 24, 2024, and updated on October 9, 2024: https://www.zoom.com/en/blog/guide-to-post-quantum-end-to-end-encryption/ (accessed October 18, 2024).

14 Zoom, "Using end-to-end encryption (E2EE) in Zoom meetings," *Zoom Support*, July 15, 2024: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065408 (accessed October 18, 2024).

Browsers

Quantum Secure: As of August 2023, **Google Chrome** deployed Kyber768 alongside the elliptic curve algorithm X25519 to establish symmetric keys in TLS, which is a networking protocol.[15] While the symmetric encryption algorithms in TLS protect data in transit, the creation of symmetric keys is vulnerable. This is why Chrome transitioned to quantum-resistant session keys. Whenever browsers like Chrome establish a connection to a website or transmit a password, for instance, the connection is protected with TLS.

As **Brave Browser** and **Microsoft Edge** are based on Chromium, the open-source version of Chrome, they also include the TLS 1.3 "hybridized Kyber support" feature that Chrome has.

Quantum Experimental: In January 2024, **Firefox** Nightly, a development version of the browser, received an update that would allow it to support post-quantum key agreement.[16] It might be rolled out to the standard version of Firefox soon.

In March 2023, a developer for the **Tor Browser** mentioned that it will transition to quantum-proof algorithms.[17] The first step was to be implemented in 2023 by breaking up larger messages into smaller messages via a method called "fragmented cells." This method would allow Tor Browser to implement quantum-resistant encryption in the future.

Quantum Insecure: While Apple has been cutting-edge in bringing post-quantum encryption to iMessage, it has been lagging when it comes to its **Safari Browser**. Safari remains inherently vulnerable.

Cloud Services

Quantum Secure: In 2020, **IBM Cloud** became one of the earliest adopters of quantum-resistant algorithms that facilitate secure communications between clients and servers. Like many other companies, it relies on a hybrid approach in which Kyber512, Kyber768, and Kyber1024 ensure that key exchanges are done in a quantum-proof manner.[18]

In June 2023, **Amazon Web Services** (AWS) stated that a variety of its services, including its AWS Key Management Service, AWS Certificate Manager, and AWS Secrets Manager TLS endpoints already deploy post-quantum-hybrid key exchange with Kyber.[19]

Quantum Experimental: **SAP** has developed a few proofs of concept to test the feasibility of a quantum-resistant algorithm roll out, but it has not yet deployed any in its systems.[20]

In September 2024, **Microsoft** proclaimed that it released support for post-quantum algorithms in its cryptographic library SymCrypt.[21]

Cisco has developed the Secure Key Integration Protocol (SKIP), which allows Cisco devices to use quantum-secure keys provided by quantum key distribution systems (QKD).[22]

Akamai Technology's **Linode** has been testing open-source implementations of post-quantum algorithms, but it has not yet taken any major steps to deploy them on a wider scale.[23]

15 Chromium, "Protecting Chrome Traffic with Hybrid Kyber KEM," *Chromium Blog*, August 10, 2023: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html (accessed October 18, 2024).

16 Cloudflare, "The state of the post-quantum Internet," *The Cloudflare Blog*, March 5, 2024: https://blog.cloudflare.com/pq-2024/ (accessed October 18, 2024).

17 Tor, "Post Quantum Cryptography," *Tor Project*, February 2023: https://forum.torproject.org/t/post-quantum-cryptography/6563/2 (accessed October 18, 2024).

18 IBM, "Introducing Quantum-Safe Crypto TLS for IBM Key Protect," *IBM Blog*, December 3, 2020: https://www.ibm.com/blog/introducing-quantum-safe-crypto-tls-for-ibm-key-protect/ (accessed October 18, 2024).

19 Amazon Web Services, "Post-quantum hybrid SFTP file transfers using AWS Transfer Family," *AWS Security Blog*, June 13, 2023: https://aws.amazon.com/blogs/security/post-quantum-hybrid-sftp-file-transfers-using-aws-transfer-family/ (accessed October 18, 2024).

20 SAP, "SAP and Quantum Technologies," *SAP News Center*, November 19, 2021: https://news.sap.com/2021/11/sap-and-quantum-technologies/#:~:text=SAP%20continuously%20analyzes%20new%20cryptographic,%2C%20data%20leaks%2C%20and%20espionage (accessed October 18, 2024).

21 Microsoft, "Microsoft's quantum-resistant cryptography is here," *Microsoft Tech Community*, September 9, 2024: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780 (accessed October 18, 2024).

22 Cisco is experimenting with securing information by relying on quantum communications and adding post-quantum cryptography to those communications networks. Cisco, "Bringing post-quantum cryptography to communications networks," *Cisco UK & Ireland Blog*, November 10, 2023: https://gblogs.cisco.com/uki/bringing-post-quantum-cryptography-to-communications-networks/ (accessed October 18, 2024).

23 Akamai, "Akamai and the Adoption of Post-Quantum Cryptography," *Akamai Blog*, April 27, 2023: https://www.akamai.com/blog/security/akamai-and-post-quantum-cryptography (accessed October 18, 2024).

Google Cloud is using the NTRU-HRSS-KEM algorithm instead of Kyber since the latter's intellectual property status is still unclear.[24] It is only using it for its internal communications, however, and has not deployed it more broadly for Google Cloud customers.

Quantum Insecure: The German company **Software AG** as well as the US-based companies **Salesforce** and **Oracle Cloud** have not yet shown any signs of experimenting with post-quantum encryption and are far from having it deployed.

Virtual Private Networks (VPNs)

Quantum Secure: On October 25, 2023, **ExpressVPN** proclaimed that it had added post-quantum resilience to its Lightway VPN protocol.[25] It uses P256_KYBER_LEVEL1 for UDP and P521_KYBER_LEVEL5 for TCP. Both UDP and TCP are data transmission protocols, which are a set of rules that lay out how data is transmitted across devices.

For its part, **MullvadVPN** announced in August 2024 that it uses quantum-proof Classic McEliece and Kyber algorithms on its WireGuard servers.[26]

At the end of September 2024, **NordVPN** launched a Linux app update that includes the first post-quantum cryptography upgrade for the Nordlynx protocol. It plans to extend this support to all its applications.[27]

Quantum Experimental: Around 2020, Microsoft released a version of **OpenVPN**, Post-Quantum Crypto VPN, which integrates post-quantum cryptography into VPN software.[28]

Quantum Insecure: While users can choose among a few companies that deploy post-quantum cryptography in their networks, a large portion of companies has been inactive on this front. Those are: **Surfshark, PIA VPN, Private VPN, CyberGhost, Windscribe, IPVanish,** and **ProtonVPN.**

POLICY RECOMMENDATIONS FOR GERMANY

We have provided the above analysis to lay out where Germany currently stands in the transition to a quantum-resilient infrastructure that relies on post-quantum encryption. While Germany's government sector proves to be slightly more advanced, its private sector is inherently vulnerable. On the other side of the Atlantic the picture is different. In the United States, a few companies have remarkably accelerated their efforts to become quantum secure. Yet, there too, many are still lagging and remain vulnerable to "harvest now, decrypt later" attacks. To begin to catch up to their international competition, German actors should take the following steps:

- **Double down on standardization** – Standardization appears to be the single most important factor for companies to accomplish the quantum transition. Most company transitions occurred after July 2022 when the US-based National Institute of Standards and Technology (NIST) chose and announced four quantum-resistant-cryptographic algorithms. In this context, efforts by the German Federal Office of Information Security (BSI) and email services provider Proton to establish a post-quantum public-key algorithm extension for the OpenPGP standard are laudable and should be doubled-down upon.

- **Just do it** – In the messaging industry, Signal and iMessage have shown that updating messaging protocols is possible. German products must follow their example and simply make the transition. Neither BWMessenger nor BundesMessenger is currently quantum secure. There is no reason why they should not be.

- **Make it easy** – When German companies enter the quantum transition, they need to avoid making quantum-proof services cumbersome to users. In MullvadVPN, users need to actively enable quantum-resistant tunnels. In the Chrome, Brave, and Edge browsers, quantum-proof features are

24 Google Cloud, "Securing tomorrow today: Why Google now protects its internal communications from quantum threats," *Google Cloud Blog*, November 19, 2022: https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms?hl=en (accessed October 18, 2024).

25 ExpressVPN, "ExpressVPN launches post-quantum protection on Lightway," *EpxressVPN News*, October 25, 2023: https://www.expressvpn.com/blog/expressvpn-launches-post-quantum-protection-on-lightway/ (accessed October 18, 2024).

26 AlternativeTo, "Mullvad introduces quantum-resistant VPN tunnels for enhanced future-proof security," August 30, 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*, April 6, 2023: https://mullvad.net/en/blog/stable-quantum-resistant-tunnels-in-the-app (both accessed October 18, 2024).

27 NordVPN, "NordVPN launches first app with post-quantum encryption support," *NordVPN Blog*, September 30, 2024: https://nordvpn.com/blog/nordvpn-linux-post-quantum-encryption-support/ (accessed October 18, 2024).

28 Microsoft, "Post-quantum Cryptography," *Microsoft Research*: (https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/ (accessed October 18, 2024).

still optional. Further, the level of risk when enabling these features is communicated too vaguely – Chrome, for example, warns users "you could... compromise your security or privacy" by doing so.[29] This does not incentivize adoption. In Zoom, quantum-proof communications require enabling end-to-end encryption, leaving users with an all or nothing option. Instead, Zoom calls should be end-to-end encrypted by default with the option of activating post-quantum encryption.

- **Increase transparency** – Companies need to make clear where they stand in the quantum transition. SAP, for instance, states that it has developed proofs of concept, but it does not provide a timeline detailing when it will deploy its quantum-proof solutions. Others are claiming that only parts of their products are quantum-resilient. NordVPN's quantum-update applies only to the Linux app; MullvadVPN's only to their desktop app and not to iOS or Android. More explanation about why these choices were made would be helpful.

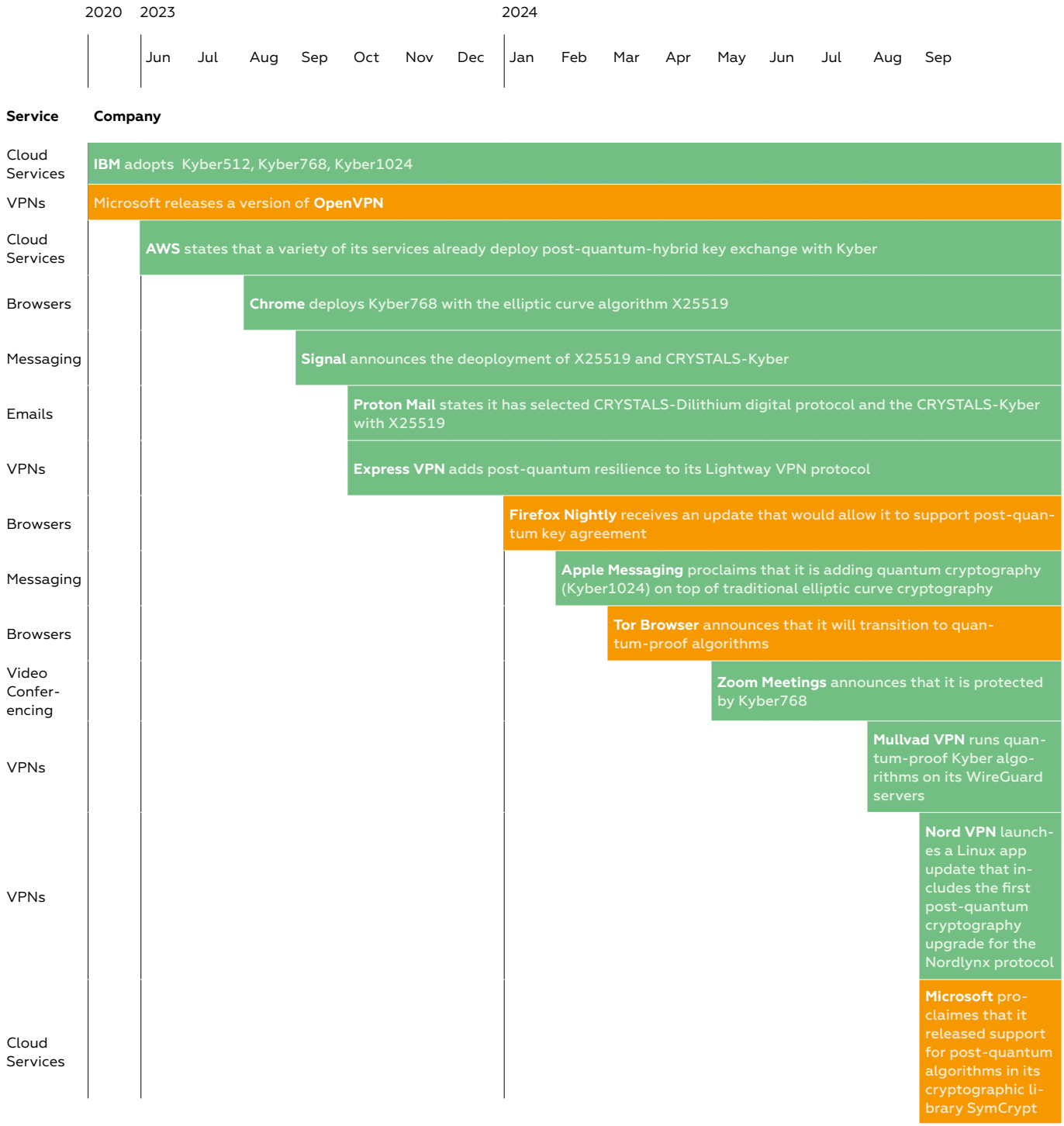
The authors would like to thank Heike Hagemeier for her insightful feedback on earlier drafts of this DGAP Policy Brief. Any errors are the sole responsibility of the authors

29 Google Chrome Administrative Templates (Computers): https://admx.help/?Category=Chrome&Policy=Google.Policies.Chrome::EnableExperimentalPolicies (accessed October 18, 2024).

APPENDIX

Timeline of the Transition to Quantum Encryption

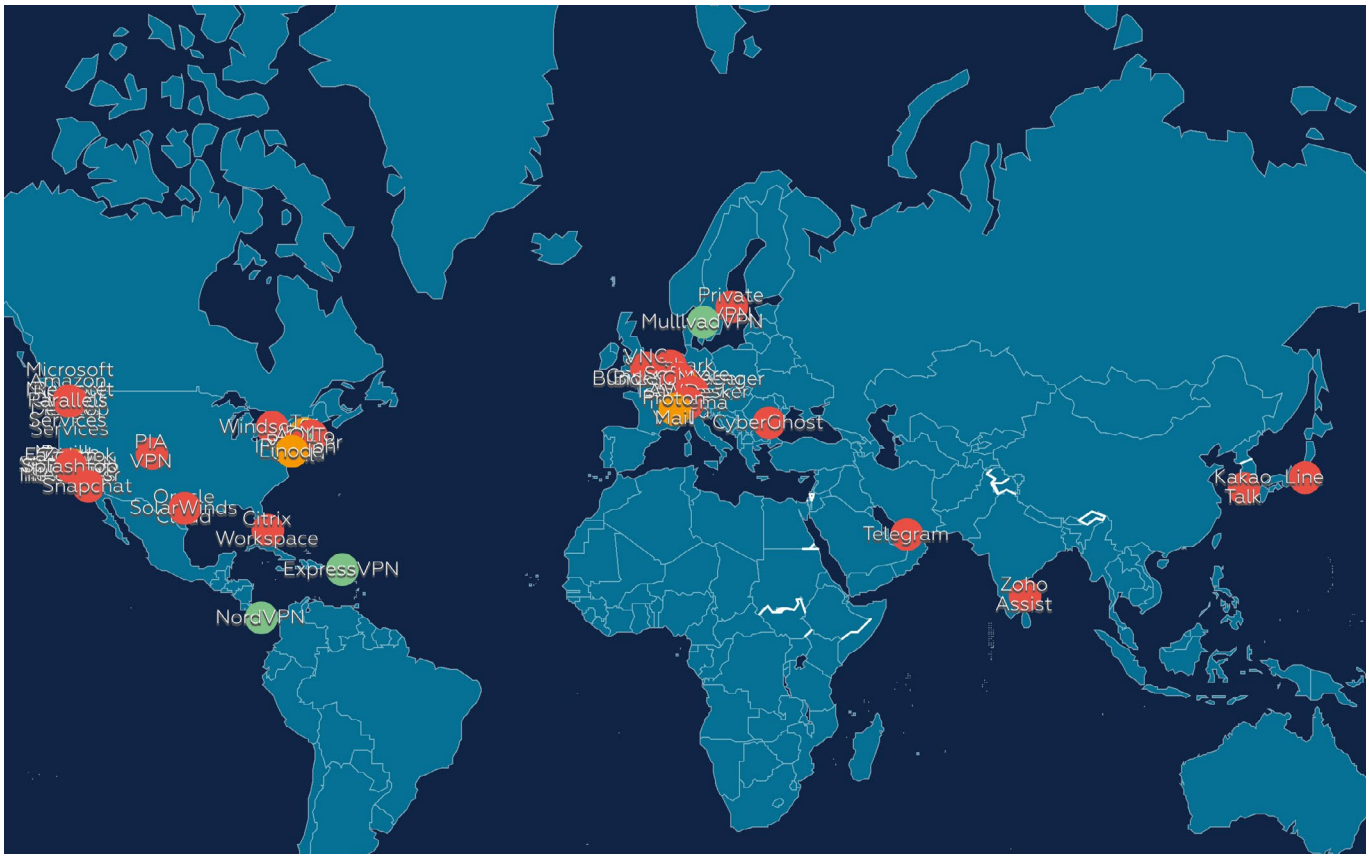
Quantum Secure
Quantum Experimental



Source: Authors' own compilation

Chart 2 – Headquarter Locations of Selected Companies

Quantum Secure
Quantum Experimental
Quantum Insecure



COUNTRY	CITY	COMPANY	PRODUCT
British Virgin Islands	British Virgin Islands	Kape Technologies	ExpressVPN
Canada	Toronto, Ontario	Windscribe	Windscribe
Germany	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
India	Chennai, Tamil Nadu	Zoho	Zoho Assist
Japan	Tokyo	Line	Line
Luxembourg	Luxembourg	Skype – Microsoft-owned	Skype
	Luxembourg	Viber	Viber
Panama	Panama City	NordVPN	NordVPN

COUNTRY	CITY	COMPANY	PRODUCT
Romania	Bucharest	CyberGhost	CyberGhost
South Korea	Jeju City	Kakao Corporation	Kakao Talk
Sweden	Gothenburg	MullvadVPN	MulllvadVPN
	Sollentuna	Private VPN	Private VPN
Switzerland	Geneva	Proton	Proton VPN
	Geneva		Proton Mail
	Pfäffikon	Threema	Threema
	Zug	Wire Swiss	Wire Bund
	Zug		Wire
The Netherlands	Amsterdam	Surfshark	Surfshark
United Arab Emirates	Dubai	Telegram	Telegram
United Kingdom	Cambridge	RealVNC	VNC Connect
United States	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

COUNTRY	CITY	COMPANY	PRODUCT
United States	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

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Helga Beck

Layout Luise Rombach, Daniel Faller

Design Concept WeDo

Author photo(s) © DGAP