The Outlook of German Companies on IT-Security and Their Readiness for Quantum Computing

Paulina Schindler

Friedrich Schiller University Jena, Germany

Abstract

Quantum computers are currently in development. As soon as they are available for widespread use, they can offer great benefits for companies. However, they can also pose dangers to information security. Because of this, protection measures are needed. To gain an insight into the outlook and knowledge of companies on quantum computing and their internal decision processes when establishing new technologies, qualitative interviews were conducted. Because not all companies know about quantum computing, the questions were designed without necessary previous knowledge in mind. Additionally, an employee of the German Federal Office for Information Security (BSI) was asked for their opinions. Many of the interviewed companies were not well informed about quantum computing and some lacked preparation of their general IT security. However, they had ideas how they could utilize such a much more powerful computer in the future. To gauge how quantum-secure measures could be implemented among companies, the companies were asked about their decision criteria when deciding on implementing a new technology. Their answers often included price and distribution, functions of the technology and external influences like other companies or guidelines from the government. To support the transition to quantum computer-safe cryptography in companies, different areas of action are examined. Supporting the availability of relevant use cases, market incubation and standards, collaboration between companies and education among them can help in pushing the spread of post-quantum security in companies in the future.

Keywords: post-quantum cryptography, decision criteria, interview

1. The advent of quantum computers

Quantum computers are currently in development. Due to their way of operating, they will be able to process tasks significantly faster than conventional computers (Ernst, Warnke and Schröter 2020; Mailloux et al. 2016). They are not yet available for widespread use and it is unclear when exactly they will be (Dyakonov 2018; Mailloux et al. 2016; Mohr et al. 2021), but they already pose a danger to data security now. The German Federal Office for Information Security (BSI) has the hypothesis that cryptographically relevant quantum computers will be available after 2030, although that date shouldn't be interpreted as a prognosis but rather as a benchmark for risk assessment (BSI 2021). Even though that date lies in the future, the benefits and dangers of quantum computers for companies are already relevant for all industries, especially in the realm of cryptography, because quantum computers will be able to crack encryption that is widely used today (BSI 2021; Mailloux et al. 2016). Many present-day widely used cryptosystems could collapse (Alyami et al. 2022). This makes a transition to new systems necessary that has a far greater scope and implications as classical security transitions (Joseph et al. 2022).

To continue to protect data, the migration to quantum secure cryptography must happen before quantum computers reach market maturity. If the migration to quantum computer safe cryptography takes too long, data that has to be kept safe for a certain time might be left unprotected when quantum computers are available (Mosca 2018). However, quantum computers are not only relevant in the future, but also already pose an active threat (Joseph et al. 2022). Attacks can be realized by storing encrypted data now and decoding it as soon as quantum computers become available, also called a store-now-decrypt-later attack (Cesare 2015; Joseph et al. 2022). Because of this, appropriate quantum-secure cryptography measures should be used sooner rather than later and strategic planning by companies should have already begun if data must be protected for more than five years or is used in the long-term planning of projects. Because of this, most companies can already be considered late (Joseph et al. 2022).

Data can be protected in the face of quantum computing by means of quantum cryptography or post-quantum cryptography (BSI 2021). While quantum cryptography works with quantum phenomena and thus is suited for quantum computers, post-quantum cryptography aims to encrypt with algorithms on classical computers in a way it can't be decrypted by quantum computers. Especially post-quantum cryptography is seen as suitable for companies because it is easier to establish in a conventional infrastructure (Joseph et al. 2022). The development of these measures and their international standardization is underway (National Institute of Standards and Technology 2022) and has already produced four algorithms that are planned to be included in future standards (NIST 2022). It is recommended to users to already take stock of their applications that use public-key cryptography to replace them later when the final standards are published. Early preparation allows companies to train their workforce and prepare their systems accordingly (Joseph et al. 2022).

The commercial market for quantum computing is still in its infancy and thus faces a lot of challenges like the difficulty of accessing quantum systems even with cloud service providers, the resulting lack of experience in companies and experienced personnel in the market, and the current lack of demand in the market (Bayerstadler et al. 2021). Because of this, companies may be prevented from developing their own quantum computer secure solutions and thus will have to rely on standardized solutions by software providers. As soon as multiple solutions become available, companies will have to choose. Exactly how this decision-making process will take place in a company is unclear. Because this security gap must be closed before quantum computers attempt to access encrypted data, companies must adopt such solutions as soon as possible. To close the information gap on corporate decision-making that determines whether to adopt such a solution, interviews were conducted with different companies.

2. Possible benefits of quantum computers for companies

The dangers associated with quantum computing may cause companies to reject it in general or only focus on the protection aspect of it. Yet, regardless of the security issue, quantum computers have great application potential in many areas that can be overlooked by companies and thus hinder market development in this area. Despite the associated uncertainties and risks, society has great hopes for the future uses of quantum computing (Ernst, Warnke and Schröter 2020). Even though quantum computers are not available yet, there are already ideas for future use cases. However, exact implementations cannot be determined yet due to the lack of availability of quantum computers. The proposed applications are widespread and not limited to certain business sectors (Piattini, Peterssen and Pérez-Castillo 2020). Because quantum supremacy allows quantum computers to process data faster than classical computers, many applications that focus on Big Data analytics could be sped up (Shaikh and Ali 2016). Especially quantum machine learning could become a promising application (Hassija et al. 2020; Outeiral et al. 2021; Ramezani et al. 2020; Srivasta et al. 2016). This is why the finance sector is expected to be part of the first sectors to profit (Herman et al. 2022). Financial problems like risk modeling, derivate pricing, fraud detection, and portfolio management are hoped to be solved (Ali, Yue and Abreu 2022; Egger et al. 2020; Ganapathy 2021; Herman et al. 2022; Srivasta et al. 2016). Quantum applications could also be used in the logistics sector with scheduling applications (Hassija et al. 2020; Srivasta et al. 2016), in the health sector for the acceleration of disease research and drug development (Ali, Yue and Abreu 2022; Srivasta et al. 2016; Zinner et al. 2022), and in the software development sector for more efficient software tests to minimize the costs of software errors (Srivasta et al. 2016). The prospect of quantum simulations (Hassija et al. 2020) is relevant for many sectors like airplane manufacturing (Srivasta et al. 2016) or chemistry (Cheng et al. 2020; Outeiral et al. 2021; Zinner et al. 2022). The conceivable scenarios for use cases of quantum computers are manifold and depend on the company under consideration. Many industries are predicted to be revolutionized by the advent of quantum computers (Ali, Yue and Abreu 2022). However, most companies may not recognize this potential. To gain insight into that, companies are asked about their plans with quantum computing.

3. Interview topics

The issues presented demonstrate the lack of available information on this topic and the urgency it presents. As many companies are already late in the preparation for quantum computers (Joseph et al. 2022), agility and quickness in research is needed to understand the current situation of companies regarding their knowledge and thoughts on quantum computing and their internal security decision-making strategies and inform them of the threat they should already be preparing for. To be able to quickly get an impression of the current situation of companies in Germany, a small sample of companies is interviewed. A total of 11 qualitative, explorative interviews on these topics were conducted, including an interview with an employee of the German Federal Office for Information Security (BSI) to gain a governmental perspective. The interviews were conducted between March and June 2022 and lasted between 20 minutes and one hour. To gain a broad insight into the views of the German corporate landscape and because of the relevancy of quantum computers for all industries, companies from different industries and of different sizes were asked to participate. To make participation more likely, their answers were anonymized. While 50 companies were asked to participate, only 10 of them were willing to. Overall, the participating companies come from the following industries: Agriculture, Automotive, Construction, Electronics and IT, (IT) Consulting of Insurance, IT security, Metal and optics manufacturing, Software development (2x), and Tax consulting.

The specific questions that the participants were asked during the interview can be found in the appendix. These questions were arranged in this order to resemble the flow of a conversation to increase understanding on the part of the participants. In addition to general questions about the company itself (questions 1-3), the interview questions can be sorted into three categories: the general status of the company's IT security (questions 4,5,8-14), knowledge and interests in the field of quantum computing (questions 6,7) and decision criteria and influences concerning the introduction of new technologies (questions 15-19). Question 20 was designed to provide the participants with the opportunity to make additional comments.

The general status of IT security in companies is often marked by limitations, especially in small and medium enterprises (BSI 2012; Dreißigacker, Skarczinski and Wollinger 2020; Ihlau and Duscha 2019). As a result, the company is less well protected against IT security threats. Because the knowledge of the participating companies on quantum computing may be limited, the related questions were abstracted to their general internal situation concerning their IT security. To gain an impression of how committed the company is to IT security, questions were first asked about the general strength of the company's focus on IT security and internal preparation in the form of guidelines. Asking about the availability of internal IT security guidelines or plans can also be a helpful component in determining the IT security preparation of a company. The initial direction of the company's focus on IT security incident prevention is revealed by the question about the perceived greatest threat to the company. The question on how the respondent keeps up to date on IT security issues aims to identify sources through which companies can be reached to inform them of emerging security incidents like the necessity to prepare for quantum computer secure cryptography. To be able to interview companies regardless of their IT security background, these questions were formulated as simply as possible.

The question of the company's basic knowledge of quantum computing was asked to determine how much the company had so far addressed it on its own. Just like with general IT security questions, the questions asked were deliberately superficial, as the companies were not expected to have any prior knowledge of quantum computing to gain a realistic insight as possible. At the same time, the associated questions could be used to raise awareness of the topic in companies. To see which areas of application for quantum computers companies see as relevant for them and if encryption is mentioned in this regard, they were asked about this also. This also made it possible to check whether the information that public agencies already provide on the danger of quantum computing has reached companies at all. This could provide an insight into the effectiveness of those measures for these companies and whether additional measures are necessary.

The questions about their concrete decision criteria and influences were used to discover paths or arguments through which companies can be reached to establish quantum computer secure cryptography measures when they are available and which criteria will be used when the decision on one standardized quantum computer safe solution must be made in the future. Because quantum computers and associated quantum computer-secure solutions are not yet available on the market and thus companies do not have decided on this topic, the questions were abstracted to reflect the company’s general internal decision-making strategies. Several questions aim in this direction to include answers from multiple perspectives. The anonymized, summed-up answers can be found in the following.

4. Responses of an employee of the BSI

To get an impression of the behaviour of the German industry in this context, an interview was conducted with an employee of the German Federal Office for Information Security (BSI). The BSI regularly issues IT security recommendations to support companies in protecting themselves in the digital realm. Especially companies with particularly sensitive data should protect themselves at an early stage.

For some companies, the issue of the codebreaking capabilities of quantum computers has caught on. This affects a large proportion of the IT security companies supported by the BSI. Some companies, especially when working with critical infrastructure, are obliged to comply with certain IT security standards set by the BSI. However, not all companies are reached with these efforts.

It is assumed that many companies deal with IT security inadequately and only react when a security incident has already occurred. Especially companies that do not come from the IT sector are less concerned with it. A particular threat to IT security in companies is that the topic is not taken seriously enough and instead only seen as an annoying obstacle due to the additional effort involved.

The criteria used to decide on a new technology are different in every company. In addition to predefined catalogues of criteria from official bodies and the reliance on certified products, more individual criteria (e.g. the degree of protection required for company data or price) can also be applied. Unfortunately, companies and consumers often do not have sufficient information about the inner workings of software (such as the encryption methods used) to make a completely informed decision.

Companies can keep up to date on security issues via conferences, publications, and news portals, to name a few. Interested companies can also feel free to contact the BSI directly or work with industry associations or cybersecurity alliances to improve their IT security.

5. Responses of the interviewed companies

General IT security (questions 4,5,8-14)

Companies were asked about their general interest in IT security and the threats they believe they are facing. To keep up to date on security issues, specialist magazines, specialist articles on the Internet like in blogs, websites, or social media, or even internal information in the company are used. Seven companies said they place greater focus on IT security, while the others do not concern themselves with the topic beyond basic security measures. Companies from industries not mainly dealing with IT as part of their products saw hacker attacks as the biggest threat to their business, especially extortion (ransomware) and data theft. However, if the company didn’t see its data as valuable enough to outsiders, data theft was seen as less of a concern. The software development and IT security companies cited human error on the part of employees as the biggest threat. However, ransomware, data theft, and using company computers for crypto mining could also be major threats, especially for SMEs.

When asked whether the company had guidelines about IT security, seven companies answered yes and three answered no.

The time it takes to introduce new technology in a company varies depending on the company, the size of the implementation, and the tasks usually performed there. Various periods ranging from days to years were mentioned. Usually, management makes the final decision whether to introduce new technology to the company, sometimes with the advice of the IT department, if available. The implementation is usually carried out by someone responsible for

IT in the company, such as the IT department or an external IT consultant. Two companies regulate implementation in such a way that the person who requested or suggested the innovation is the one to implement it as a specialist.

Knowledge about quantum computing (questions 6,7)

The companies were asked whether they could imagine quantum computing becoming relevant for them and in what form. The company in the agriculture industry indicates that future performance improvements would be useful for real-time data processing in autonomous processes. A company in the software development sector sees the potential of quantum computers in the long term rather than the medium term. Stronger keys in connecting internal solutions to cloud computing and as a boost for in-house machine learning solutions are seen as conceivable. Several companies also address the topic as relevant for encryption. A company from the software development sector mentions the danger of storing encrypted data now and decrypting it later in this context. The company from the insurance industry describes quantum computers as useful for processing larger amounts of data fast but currently considers them unprofitable for smaller companies. The rest of the interviewed companies do not consider quantum computing to be relevant at present or describe it as a topic to be considered later.

Asked about the possible codebreaking abilities of quantum computers, none of the companies had studied it in any detail yet. This indicates a significant information gap on the part of the companies, which may inhibit the company's preparation for the advent of quantum computing and thus significantly jeopardize the company's internal data.

Criteria and influences for the decision to implement a new technology (questions 15-19)

A large proportion of the companies interviewed do not have a fixed, written set of criteria that are used to decide whether to introduce new technologies. Nevertheless, they were able to provide information on what criteria they typically use or would use. Since the answers of the companies showed similarities in topics, their answers could be sorted into three subcategories (price and distribution, functions of the technology in question and external influences) after the interviews were conducted to improve readability.

Price and distribution:

Six companies first mention the individual benefit and added value, which would have to be weighed against the costs. Eight of the companies placed particular emphasis on the costs incurred, whether for licensing or for the subsequent service. Especially when a solution is offered by several providers, the cost comparison is important. Companies from the IT security sector, software development sector and the electronics and IT sector also point out that it is not only the price that is relevant but also information about the distributing company. For example, the country of origin (and thus also the local legal situation) is also of interest. The metal and optics manufacturing company and the tax consulting company want to check by its existing reputation in the market whether the distributing company is reliable. A large company that has been in existence for several years and already successfully serves other customers is considered a reliable partner. The company in the construction industry is also concerned about the size of the distributing company - if the number of employees is too small, there is a fear that it will not be able to provide sufficient support and respond quickly to problems. In general, the service and support offered (and also its duration) are relevant criteria for five of the interviewed companies.

Functions of the technology:

The specific functions of the technology under consideration and how they affect the company (e.g. fit with its systems, adaptability to its requirements, administration options) were given as the object of consideration by nine of the companies surveyed. The five companies whose main business is IT placed a particular focus on security-related features.

External influences:

When deciding on a software solution, companies from the agricultural sector, metal and optics manufacturing, and the software development sector also take their cue from other companies that are already using one. If other companies use it and are satisfied, they consider adopting it, too.

Four companies cite external requirements as a criterion, whether from the government, which specifies concrete technology measures or from partner companies or major customers, who, for example, require special software for communications. Recommendations from external IT consultants can also be relevant here. Six of the companies surveyed mention influence by government regulations, and six companies also mention pressure from other companies (such as customer specifications or specifications by a parent company). When asked about the influence of external guidelines, six companies indicated that it was large (Tax consulting, IT security, Electronics and IT, Metal and optics manufacturing, Construction, and Software development). Three companies indicate a medium influence (Agriculture, Automotive, (IT) Consulting of insurances). A company from the software development industry indicated that there was no influence.

6. Pushing the spread of post-quantum security

Bayerstadtler et al. suggest three areas of action that can be used to accelerate the spread of quantum computing-related technologies: The availability of use cases and references in the industry, collaboration between companies, academia, and policymakers, and the initiation of a market for quantum computing technologies. Education and trained personnel and existing standards can work as enablers (Bayerstadler et al. 2021).

Use cases

The interviewed companies showed that they did have a few ideas about how quantum computing could be used to profit their company. Incentivizing such ideas from the governmental side could convince more companies to research the topic of quantum computing and how to protect themselves in this new situation. As more companies become interested in this topic, demand in the market may rise and incentivize even more companies to adapt.

Market incubation and standards

Through the dissemination of use cases, demand in the market could also be affected positively. As soon as the providers of standardized security solutions focus on the issue of security in the face of quantum computers, they should be supported in the dissemination of their products to protect companies without the resources to create their own solution early. The contribution of quantum secure standards by governmental agencies like the BSI can enable this even more and thus should be followed up on.

The criteria companies use to decide on a new technology could be used in this regard to provide a solution that is attractive to many companies. The responses collected from the interviewed companies show similarities in the criteria they use to assess new technology. In particular, the price is important to them, which must be weighed against the benefits. IT-savvy companies also considered more security-related issues, while this did not seem relevant for companies less involved with IT. To compensate for a lack of knowledge about the technology under consideration, the disseminating source is assessed by some companies for its trustworthiness.

Collaboration

Collaboration with external forces can help a company to adopt quantum secure solutions more easily and spread them in the market. The government, customers, or other companies can exert a great deal of influence on companies. They can serve both as a model to be followed and add pressure through demands that must be considered. Governmental agencies like the BSI and business associations could use their capabilities to be a positive influence on the preparation of IT security in the face of quantum computing in companies.

Education

The interviews reflected especially a lack of education about quantum computing because none of the companies surveyed had yet studied quantum computers and the security threat they can pose in detail. This shows that the governmental efforts to inform companies of the present danger could not reach these companies.

The perceived greatest IT security threat differed depending on whether the company was more or less involved with IT in its main business. While companies more involved with IT mainly cited human internal errors as a threat, less IT-related companies cited external attacks as the most threatening. Generally, IT-related companies tended to give the impression that they had prepared for IT security threats more than other companies surveyed.

To increase the effectiveness of the spread of information about quantum computers to companies, there should be additional efforts. While the BSI has already started to do so by publishing relevant papers (e.g. (BSI 2021), the companies surveyed could not be reached by them at all. The knowledge about the already active danger of quantum computers can thus not be expected to be predominant in the market. Through the communication channels identified during the interviews, such as the spread of education through blogs, social media, or magazines, the dissemination of information by the BSI and other official bodies should be intensified to reach more companies more quickly.

The collected answers can be used to get insight into the situation of the interviewed companies even though the sample is rather small and thus not representative. Because the interviewed companies come from different industries and the representatives of the companies surveyed in some cases come from different departments or management positions, the comparability of the answers can be limited. However, this diversity in terms of the source of information, in turn, ensures the broadest possible insight into the current situation of companies in the market. The exploratory, personal nature of the conversations, which also allows for follow-up questions and comprehension-aiding explanations, enables a multidimensional view of a company's situation. The collected answers are suitable for painting a picture of the working reality of various companies in Germany and how they embrace technology innovations and how the status of their IT security is. This way, new aspects that have not yet been explored in previous research could be followed up on. The fact only a fraction of contacted companies was willing to participate in the interviews shows that a lot of companies still do not concern themselves enough with this important topic. The risk quantum computers can present to them is underestimated, more so when a person lacks knowledge about it (Lowrance 1980).

The advent of quantum computers is a development that should be taken seriously by all market participants. To keep data safe, quantum computer-secure solutions should be offered and established as soon as possible. The safe, standardized build-up of the market, the associated education of companies and people, and the continued collaboration between government, companies, and academia are paramount for this. In the meantime, companies should implement crypto-agility in their security systems and begin planning for post-quantum cryptography (Joseph et al. 2022).

Appendix – Interview questions

1. Aus welcher Abteilung stammen Sie? *[Which department are you from?]*

2. Was ist das Kerngeschäft Ihres Unternehmens? *[What is the core business of your company?]*

3. Welcher Branche würden Sie Ihr Unternehmen zuordnen? *[Which industry would you classify your company in?]*

4. Wie sehr interessiert sich Ihr Unternehmen für IT-Sicherheit? *[How interested is your company in IT security?]*

5. Existieren in Ihrem Unternehmen Leitfäden zum Thema IT-Sicherheit? *[Does your company have guidelines on the subject of IT security?]*

6. Denken Sie, dass Quantencomputing für Ihr Unternehmen ein relevantes Thema werden kann? Wenn ja, in welcher Form? *[Do you think quantum computing can become a relevant topic for your company? If so, in what form?]*

7. Haben Sie sich schon einmal mit der Gefährdung durch Codebrecherfähigkeiten von Quantencomputern beschäftigt? *[Have you ever considered the threat posed by codebreaking capabilities of quantum computers?]*

8. Wie halten Sie sich in Fragen Sicherheit auf dem Laufenden? *[How do you keep up to date on safety issues?]*

9. Was ist Ihrer Ansicht nach die größte Bedrohung für Ihre IT-Sicherheit? *[What do you think is the biggest threat to your IT security?]*

10. Wie häufig werden in Ihrem Unternehmen neue Technologien/Softwares eingeführt? *[How often are new technologies/new software implemented in your company?]*

11. Wer entscheidet über die Einführung? *[Who decides on the implementation?]*

12. Auf welcher Basis wird über eine Einführung entschieden? *[On what basis is a decision made about implementation?]*

13. Wer führt die Einführung durch? *[Who carries out the implementation?]*

14. Wie lange dauert ein solcher Einführungsprozess ungefähr? *[Approximately how long does such an implementation process take?]*

15. Gibt es einen konkreten, festgeschriebenen Kriterienkatalog für die Auswahl neuer Software? *[Is there a specific, fixed catalog of criteria for the selection of new software?]*

16. Welche Auswahlkriterien nutzen Sie, um sich für Software zu entscheiden? *[What selection criteria do you use to decide on software?]*

17. Welches Kriterium ist davon das wichtigste für Sie? *[Of these, which criterion is the most important to you?]*

18. Wie groß ist der Einfluss externer Vorgaben? (z.B. staatlich, andere Unternehmen) *[How great is the influence of external requirements? (e.g. governmental, other companies)]*

19. Gibt es noch sonstige Faktoren, die Sie für relevant halten? *[Are there any other factors that you think are relevant?]*

20. Haben Sie noch etwas hinzuzufügen? *[Do you have anything to add?]*

References

Ali, S., Yue, T., & Abreu, R. (2022). When software engineering meets quantum computing. *Communications of the ACM*, *65*(4), 84–88. https://doi.org/10.1145/3512340

Alyami, H., Nadeem, M., Alosaimi, W., Alharbi, A., Kumar, R., Kumar Gupta, B., Agrawal, A., & Ahmad Khan, R. (2022). Analyzing the Data of Software Security Life-Span: Quantum Computing Era. *Intelligent Automation & Soft Computing*, *31*(2), 707–716. https://doi.org/10.32604/iasc.2022.020780

Bayerstadler, A., Becquin, G., Binder, J., Botter, T., Ehm, H., Ehmer, T., Erdmann, M., Gaus, N., Harbach, P., Hess, M., Klepsch, J., Leib, M., Luber, S., Luckow, A., Mansky, M., Mauerer, W., Neukart, F., Niedermeier, C., Palackal, L., . . . Winter, F. (2021). Industry quantum computing applications. *EPJ Quantum Technology*, *8*(1). https://doi.org/10.1140/epjqt/s40507-021-00114-x

BSI. (2012). *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen*. [IT security level in small and medium enterprises]. Bundesministerium für Wirtschaft und Technologie.

BSI. (2021). *Kryptographie quantensicher gestalten*. [Making cryptography quantum secure]. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf?__blob=publicationFile&v=5

Cesare, C. (2015). Online security braces for quantum revolution. *Nature*, *525*(7568), 167–168. https://doi.org/10.1038/525167a

Cheng, H.-P., Deumens, E., Freericks, J. K., Li, C., & Sanders, B. A. (2020). Application of Quantum Computing to Biochemical Systems: A Look to the Future. *Frontiers in Chemistry*, *8*, 587143. https://doi.org/10.3389/fchem.2020.587143

Dreißigacker, A., Skarczinski, B. von, & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019*. [Cyberattacks against companies in Germany: results of a representative company survey 2018/2019]. Forschungsbericht Nr. 152. Kriminologisches Forschungsinstitut Niedersachsen e.V.

Dyakonov, M. (2018). *The Case Against Quantum Computing*. https://spectrum.ieee.org/the-case-against-quantum-computing

Egger, D. J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., Simonetto, A., Woerner, S., & Yndurain, E. (2020). Quantum Computing for Finance: State-of-the-Art and Future Prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1–24. https://doi.org/10.1109/TQE.2020.3030314

Ernst, C., Warnke, M., & Schröter, J. (2020). *Der Quantencomputer – ein zukünftiger Gegenstand der Medienwissenschaft?* [The quantum computer - a future subject of media science?]. Advance online publication. https://doi.org/10.25969/mediarep/14866

Ganapathy, A. (2021). Quantum Computing in High Frequency Trading and Fraud Detection. *Engineering International*, *9*(2), 61–72. https://doi.org/10.18034/ei.v9i2.549

Hassija, V., Chamola, V., Goyal, A., Kanhere, S. S., & Guizani, N. (2020). Forthcoming applications of quantum computing: peeking into the future. *IET Quantum Communication*, *1*(2), 35–41. https://doi.org/10.1049/iet-qtc.2020.0026

Herman, D., Googin, C., Liu, X., Galda, A., Safro, I., Sun, Y., Pistoia, M., & Alexeev, Y. (2022, January 8). *A Survey of Quantum Computing for Finance*. https://arxiv.org/pdf/2201.02773

Ihlau, S., & Duscha, H. (2019). *Besonderheiten bei der Bewertung von KMU*. [Particularities in the valuation of SMEs]. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-18675-3

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature*, *605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2

Lowrance, W. W. (1980). The Nature of Risk. In R. C. Schwing & W. A. Albers (Eds.), *Societal Risk Assessment* (pp. 5–17). Springer US. https://doi.org/10.1007/978-1-4899-0445-4_1

Mailloux, L. O., Lewis II, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals. *IT Professional*, *18*(5), 42–47. https://doi.org/10.1109/MITP.2016.77

Mohr, N., Ostojic, I., Heid, A., Pautasso, L., & Biondi, M. (2021). Die wundersame Welt der Quantencomputer: ein Wegweiser. [The wondrous world of quantum computing: a guide]. *Digitale Welt*, *5*(2), 6–9. https://doi.org/10.1007/s42354-021-0328-6

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

National Institute of Standards and Technology. (2022). *Post-Quantum Cryptography*. https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST. (2022). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Outeiral, C., Strahm, M., Shi, J., Morris, G. M., Benjamin, S. C., & Deane, C. M. (2021). The prospects of quantum computing in computational molecular biology. *WIREs Computational Molecular Science*, *11*(1). https://doi.org/10.1002/wcms.1481

Piattini, M., Peterssen, G., & Pérez-Castillo, R. (2020). Quantum Computing. *ACM SIGSOFT Software Engineering Notes*, *45*(3), 12–14. https://doi.org/10.1145/3402127.3402131

Ramezani, S. B., Sommers, A., Manchukonda, H. K., Rahimi, S., & Amirlatifi, A. (2020). Machine Learning Algorithms in Quantum Computing: A Survey. In *2020 International Joint Conference on Neural Networks (IJCNN): 2020 conference proceedings* (pp. 1–8). IEEE. https://doi.org/10.1109/IJCNN48605.2020.9207714

Shaikh, T. A., & Ali, R. (2016). Quantum Computing in Big Data Analytics: A Survey. In *2016 16th IEEE International Conference on Computer and Information Technology - CIT 2016, 2016 6th International Symposium on Cloud and Service Computing - IEEE SC2 2016, 2016 International Symposium on Security and Privacy in Social Networks and Big Data - SocialSec 2016: Proceedings : 7-10 December 2016, Nadi, Fiji* (pp. 112–115). IEEE. https://doi.org/10.1109/CIT.2016.79

Srivasta, R., Choi, I., Cook, T., & NQIT. (2016). *The Commercial Propects for Quantum Computing*. NQIT. https://nqit.ox.ac.uk/content/commercial-prospects-quantum-computing.html

Zinner, M., Dahlhausen, F., Boehme, P., Ehlers, J., Bieske, L., & Fehring, L. (2022). Toward the institutionalization of quantum computing in pharmaceutical research. *Drug Discovery Today*, *27*(2), 378–383. https://doi.org/10.1016/j.drudis.2021.10.006