A Comprehensive Tutorial on Cybersecurity in Quantum Computing Paradigm

Uttam Ghosh, *Senior Member, IEEE,* Debashis Das, *Student Member, IEEE,* and Pushpita Chatterjee, *Senior Member, IEEE*

***Abstract*—Quantum computing has the potential to revolutionize computing by solving problems that classical computers cannot solve efficiently. However, it also poses a significant threat to cybersecurity. Quantum computers can break many of the encryption methods that are currently used to protect sensitive information. This includes breaking public-key encryption, decrypting symmetric keys, forging digital signatures, and stealing private keys. To mitigate this threat, efforts are underway to develop new encryption methods that are resistant to quantum attacks. Cybersecurity is a constantly evolving field, and as quantum computing continues to develop, new strategies and tools will be needed to defend against cyber threats. By staying informed and proactive, individuals and organizations can help ensure the security of their digital assets in the face of this new paradigm. In this paper, we will explain what quantum computing is and look at how it might be used in cybersecurity. Quantum computing could make cybersecurity less safe, so we talk about cybersecurity threats to learn more about them. We also introduce several quantum attacks and their countermeasures. Finally, we provide quantum approaches to cybersecurity concerns.**

***Index Terms*—Quantum Computing, Cybersecurity, Advanced Cryptography, Post-quantum Security, Quantum key distribution, Cyber threats**

I. Introduction

Especially on the heels of digital transformation, the current technological stack is unquestionably evolving at breakneck speed. Enterprises are always looking for new ways to be innovative and use cutting-edge technology to move all of their business operations forward. Even though computers can do so much now, there are still some problems to solve [1]. Encryption, for instance, is a fundamental component of cybersecurity for many firms. Encryption often requires solving math problems that computers can't do. Experts in the field say that even with the processing power of computers today, it will be decades or even thousands of years before these mathematical puzzles are solved. However, quantum computing [2] is shifting the focus of the discussion in a new direction. With the arrival of quantum computing, the world may be able to solve some of its most important computing problems. Quantum computers [3], which have computing capacity based on the power of the known universe, will do mathematical operations 158,000,000 times quicker than ordinary computers [4]. They can finish a calculation in four minutes that would take computers of today thousands of years to finish.

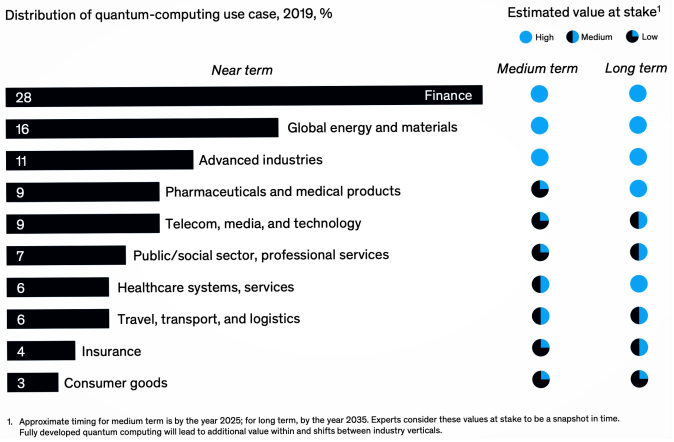

Fig. 1: Use cases of Quantum Computing [5].

Quantum computing could be used in a wide range of fields and businesses, as shown in Fig. 1, from making credit risk analysis more accurate to reducing carbon and other greenhouse gas emissions through better routing. In light of this, the federal government of the United States has recently authorized a spending plan of $280 billion for research that includes quantum computing as one of the most important areas in which to invest those funds [4]. The use of quantum computing in some fields, such as cryptography and cybersecurity, will result in a shift in the way organizations work today. Due to the potential damage that may be caused by bad actors using quantum computing, researchers at HUB Security feel that the post-quantum world must be ready to begin as soon as possible [6]. So, HUB Security is getting ready to take advantage of this trend by saying that its Quantum Cure ransomware solution guarantees that business backups are always safe, clean, and willing to use [7].

In this day and age of information technology (IT) and artificial intelligence (AI) [8], the main goal is to make sure that any software or online apps being used are safe. When done at the beginning of a process, finding evidence of security gives significant results that help one understand how to handle security leftovers to get the best results possible. A different security system uses a variety of procedures and algorithms to make sure the program is safe. Security estimation is one of the

Uttam Ghosh is with the Department of Computer Science and Data Science, Meharry Medical College, TN, USA, email: ghosh.uttam@ieee.org.

Debashis Das is with the Department of Computer Science and Engineering, University of Kalyani, Kalyani, India, email: debashis.das@ieee.org.

Pushpita Chatterjee is with the Department of Electrical Engineering and Computer Science and Engineering, Howard University, Washington, DC, USA, emial: pushpita.c@ieee.org.

Corresponding author: Debashis Das, debashis.das@ieee.org.

most important parts of evaluating, administering, and managing security to make it work better. It's important to know that a security assessment done early on in the development process can help find unique worms, risks, vulnerabilities, and threats.

Contribution of the work This article will discuss the definition of quantum computing as it relates to cybersecurity as well as characterize quantum computing. The main contribution of this paper is presented as follows:

- We give an overview of quantum computing, and how it can affect cybersecurity issues is discussed.
- We demonstrate a few security problems that exist in quantum computing solutions.
- We present several quantum computing solutions in the context of cybersecurity in different areas.
- We show how quantum computing could be used in the future to make cybersecurity solutions better than they are now.

The remainder of this paper is organized as follows. Section II gives the existing security issues in the ecosystem of quantum computing. Applications of quantum computing for cybersecurity solutions are stated in Section III. Section IV depicts several quantum threats in cybersecurity. The possible approaches of quantum computing in cybersecurity are given in Section V. Section VI introduces some future research aspects in quantum-based cybersecurity solutions. Finally, the paper is concluded in section VII.

II. Quantum Computing and Security Ecosystems

The cybersecurity community around the world is quickly learning more about the possible bad effects of the current technological arms race. This is because quantum computing has the potential to mess with the cryptographic foundations of the infrastructure, which are very important to the system as a whole if they are used in an unethical way. Businesses and the digital economy as a whole rely heavily on this underlying infrastructure. Also, the community needs to act right away to make sure that worries about safety and getting a competitive edge don't end up being big problems that stop quantum technology from having all of its potentially revolutionary effects. This can only be done by taking immediate action. As part of the World Economic Forum Center for Cybersecurity's Future Series, a recent conference brought together well-known experts in technology, security, and policy from all over the world to talk about the strategic cybersecurity concerns that quantum technology raises [5]. Certain problems can only be solved with the concerted effort of the whole global community working together.

Decryption Capability Public-key cryptography is "doomed to fail" because a powerful and error-corrected quantum computer would be able to calculate it too quickly. This would put at risk the technology that is used to protect many of today's most important digital systems and activities. In this case, key exchanges, encryption, and digital signatures, which are used to protect financial transactions, secure communications, e-commerce, identification, and electronic voting, would all be useless.

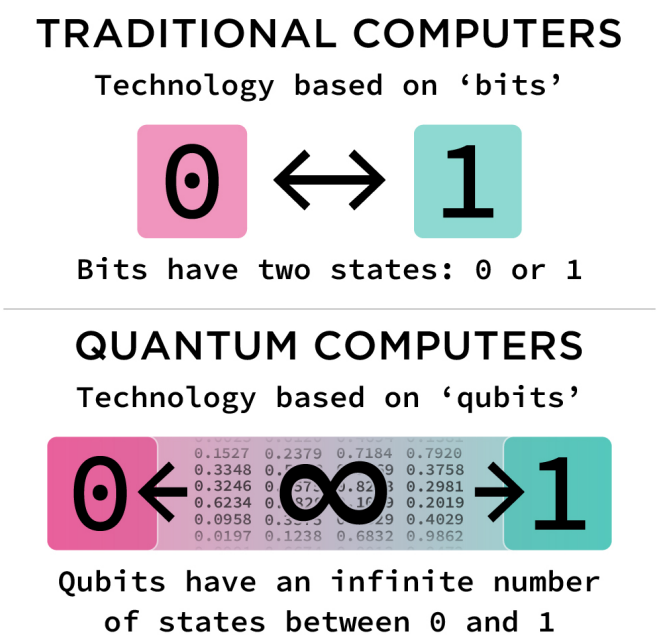

Fig. 2: Traditional computers vs quantum computers [9]

Digitization of Infrastructures Companies and governments may no longer be able to guarantee that the financial transactions and data they rely on will be available, kept private, and correct. In the end, all of our data could be in danger because of this. There is a clear possible future danger that is relevant to the risk choices that are being made today in traditional computers (shown in Fig. 2), while the timetable and potential repercussions are now the subjects of discussion among technology and security experts. This is particularly the case in industries that are now rolling out sensitive data and systems that have lengthy lifespans, such as healthcare, satellites, vehicles, and industrial control systems, all of which might be in operation for decades, if not longer.

Globalizing of Ecosystem The global ecosystem has produced a variety of shared infrastructures, each of which has dispersed ownership and control in the process of rolling out more and more of them. In cases where these systems have a long history, there is already a collective reliance on cryptography that may be vulnerable to attack, as shown in Fig. 3. It is happening at a time when hyperconnectivity is making shared architectures, networked systems, and business models that depend on each other more common. Implementations of public-key cryptography, like SSL, TLS, and HTTPS, help keep infrastructure safe, including the Internet's architecture. These implementations are used all over the world and could be attacked.

Geopolitics of Quantum Computing Unlocking the potentially transformative value of quantum technology in the larger economy may be met with significant obstacles due to national security concerns regarding sovereignty and the need to maintain control over strategic capabilities. These

Cryptographic algorithm	After quantum computing
AES-256	Secure but weakened
SHA-256	Secure but weakened
RSA	No longer secure
ECDSA	No longer secure
DSA	No longer secure

Fig. 3: Breaking down the security levels of cryptographic algorithms [10].

obstacles may make it difficult to realize the full potential of quantum technology. These difficulties might constitute significant impediments. As a result of quantum technology, which has the potential to completely change the game in terms of both national security and the information race, there is a real risk that competition will interfere with international collaboration and further widen existing gaps in security and industrial capability. This risk arises as a direct consequence of the fact that quantum technology possesses the potential to completely change the game. Several nations have already included quantum technology on their lists of restricted commodities, and governments all over the globe are investing a significant amount of money in the research and development of their very own quantum technologies and knowledge to keep up with the competition. There is no known history of complicated security breaches that have been reported. These include the ability to explain how quantum algorithms made decisions (explainability), verifying that the algorithms do what they say they do and are not biased by nature (verification), and certifying the results that they produce. Other examples include being able to explain how quantum algorithms made decisions (explainability) (certification). The capacity to convey how quantum algorithms have arrived at their conclusions is also included in this category. [Case in point:] Even though this issue is linked to artificial intelligence (AI), there are other, more profound hazards, such as the potential of abuse by criminals and other players in the world. These risks might have a significant impact on the future.

Cryptography and Quantum Computing Quantum computing speeds up the process of breaking prime numbers into their factors [11]. It means that computers with this technology can easily break cryptographic keys by quickly calculating or searching for secret keys in a very thorough way. It makes it possible for these computers to easily crack passwords. Traditional computers would find it impossible to do a certain task, but when it's done on a new computer, it's easy as pie, which makes the cryptographic techniques that are used everywhere less secure. In the not-too-distant future, quantum computing will make even the most secure cryptographic methods much less useful, and some will stop working at all as a security measure. The real-world effects of weaker cryptographic algorithms [12] could become very important if quantum computing keeps getting better and moves out of the realm of research labs and academic papers. It is anticipated that over the next decade, these devices would be accessible to government agencies and huge enterprises throughout the globe, providing them with access and power that have never been seen before. Quantum computing could be a huge step forward for humanity, but it could also be a big problem for the algorithms that keep us safe online.

III. Cybersecurity and Quantum Computing

The research is directly about how to keep traditional ways of technology, communication, and information safe while keeping their adaptability in the post-quantum era. It is one of the scientific fields that is receiving a lot of attention right now. The concept that they should be placed in a quantum-safe state is a broader one [13]. Since we just started our trip, we still have a long way to go before we can say for sure that we have answers that can be taken as final. Quantum applications are used in many other ways, like making quantum random numbers, making quantum signatures, the Byzantine agreement, quantum flip-the-coin, secure electronic voting, secure multi-party computing, and so on [14].

Quantum Device We now have something referred to as a "quantum device," and it may be used to improve the safety of conventional communication primitives. One such example is the distribution of quantum keys (QKD) [15]. The notion that two honest people may have a shared random secret key that is only known to them is where the concept of QKD originates from. An opponent must first be able to read the key before he or she can intercept the secret random key. After a quantum state has been "read" or measured, it will "collapse" into one of the classical states, which will be either 0 or 1. Because of this, any such hostile penetration causes something strange to happen in the whole system, which can be encountered.

Quantum Fingerprints There are several other ways in which a quantum device could pave the way for our regular security systems and primitives. One such approach is via the use of quantum fingerprints. One way to think of it is as a method of producing a string that is similar to the traditional cryptographic hash functions that we use, but it makes use of a quantum computer.

Secret Key Cryptography People think that there are several security methods available right now that could be useful in the post-quantum world. One such technology is called secret-key cryptography. The quantum feature of the quantum computer, on the other hand, creates a new security vulnerability that must be addressed. The superposition assault is one example of this kind of attack. To explain it more simply, superposition is a quantum property in which a qubit, which is the name given to a bit in a quantum computer, may either have the value 0 or the value 1, or it can have a combination of the two. As soon as you measure the qubit, it will either collapse to the classical value of 0 or the classical value of 1. Now, a person who has access to the quantum computer oracle could learn the superposition ciphertexts of some plain text and then use a different algorithm to decipher the superposition (without directly measuring the superposition ciphertext) to learn about the cryptosystem.

Computational security Quantum computers will help with computing in a lot of different ways, from huge exponential benefits to smaller quadratic or even constant benefits [16]. These advantages will vary depending on the nature of the issue. When these devices become available, it makes sense that people will want to use the extra processing power for things that also need privacy and security. To put it another way, we are looking for secure protocols for quantum computing. Security ideas like authentication and encryption, as well as more complicated ideas like computing on encrypted data and secure multiparty computation, would need to be changed to work with quantum information and computation. This includes concepts that are more complex than authentication and encryption [17]. For this kind of question to have any meaning, we will first need to build quantum computing systems on a large enough scale to make real gains in computing power that can be used to solve everyday problems. At the moment, this is not the case. However, since it is expected that we will soon cross the classical simulation limit (having real quantum computers that are bigger than those that can be simulated by classical supercomputers), we are entering a time when real quantum speedups will eventually be possible. It's possible that we won't have to wait too much longer before performance improvements can be applied to crucial daily concerns [18].

Post-Quantum Encryption Quantum computing is expected to change a lot of businesses, especially the financial sector, but it will also change how we keep our computers safe [19]. Quantum computing probably won't be widely used until 2030 or later, but businesses should start getting ready for it now. Because it is expected that quantum computers will someday be capable of factoring prime numbers used with asymmetric encryption algorithms, which form the core of existing data security systems, organizations need to reevaluate their cryptography systems as soon as possible. The conventional method of encrypting information involves the manipulation of very large prime integers. Modern computers have a hard time deciphering these numbers due to their complexity. But since the quantum computer will be much faster at deciphering such complicated data, a new generation of encryption algorithms that can't be broken by quantum computing is needed to prevent security breaches in the business world that could be very bad [20].

Post-quantum Cryptography There is no quantum computer that can handle the huge number of qubits that would be needed to do the factoring that would be needed to break the current security protocol. This is because there is no such thing as a quantum computer. However, it is anticipated that this will alter over the next ten to twenty years, which would place firms, especially in the financial sector, in a more precarious position. Therefore, scientists, policy officials, and cybersecurity specialists are focusing their attention on the development of post-quantum cryptography (PQC) to overcome these anticipated challenges [19].

IV. Quantum Threats to cybersecurity

Quantum computing has the potential to revolutionize the world of computing by solving problems that classical computers cannot solve efficiently. However, it also poses a significant threat to cybersecurity because it can break many of the encryption methods that are currently used to protect sensitive information. Table I depicts several existing quantum threats in cybersecurity and possible countermeasures.

A big part of modern encryption is based on mathematical formulas that would take computers too long to figure out if they tried. Consider multiplying, for instance, two huge integers in your head right now to make this process easier. It is not difficult to calculate the product, but it is a far more difficult task to begin with the huge number and factor it into its two prime numbers. On the other hand, a quantum computer would have no trouble factoring those integers and breaking the encryption. Peter Shor invented a quantum method that he fittingly titled "Shor's algorithm [21]." This technique calculates big numbers very quickly and effortlessly, much more so than a traditional computer. Since that time, researchers have been hard at work constructing quantum computers that can factor numbers that are ever more complex.

Many encryption methods, such as RSA and elliptic curve cryptography, rely on the fact that it is difficult to factor large numbers. However, quantum computers can solve this problem using Shor's algorithm, which means that they can break these encryption methods in a fraction of the time that classical computers would take.Symmetric encryption, which is used to encrypt data in transit, relies on a shared secret key that both the sender and receiver know. However, quantum computers can use Grover's algorithm to search through all possible keys much faster than classical computers can, which means that they can potentially decrypt messages that were encrypted using symmetric encryption.Digital signatures are used to verify the authenticity of a message or document. However, quantum computers could use Grover's algorithm to find collisions in hash functions, which would allow them to forge digital signatures.Quantum computers could use a technique called quantum key distribution (QKD) to intercept the transmission of a private key between two parties without being detected. This would allow an attacker to steal the private key and decrypt any messages that were encrypted using that key. Overall, quantum computing poses a significant threat to cybersecurity. As quantum computers become more powerful and widespread, it will be necessary to develop new encryption methods that are resistant to quantum attacks

As the pace of advancement in quantum computing research continues to pick up speed, it is hard to rule out the potential that such a computer may be developed within the next three to five years. As one example, at the beginning of this year, researchers from Google and the KTH Royal Institute of Technology in Sweden came out with "a more efficient technique for quantum computers to execute the code-breaking operations, cutting the resources they require by orders of magnitude [35]." The results of their study, which

TABLE I: **Quantum attacks and countermeasures**

Author / Ref	Year	Attack Type	Target Area	Countermeasures
Mogos [22]	2015	Intercept-Resend Attack	Quantum Key Distribution	Binding the leakage
Gaidash *et al.,* [23]	2016	photon-number splitting attack	Quantum key distribution system	Watchdogs (superlinearity loophole)
Lutkenhaus [24]	2000	Individual Attack	realistic quantum key distribution	Addition or modification in hardware/software
Zhou *et al.,* [25]	2010	Individual Attack	BBM92 Protocol	Privacy amplification
Iwakoshi [26]	2021	Collective Attacks	Quantum key distribution system	Quantifying information
Ferenczi *et al.,* [27]	2007	Calibration Attacks	Continuous Variable Quantum Key Distribution	Long-distance transmission of keys
Pirandola *et al.,* [28]	2009	Coherent Attacks	Continuous Variable Quantum Key Distribution	Long-distance transmission of keys
Qi *et al.,* [29]	2005	Time-shift attack	Quantum key distribution system	Constant time string comparison
Iwakoshi [26]	2021	Plaintext Attacks	Quantum key distribution system	Performing higher privacy amplification
Qi *et al.,* [30]	2021	Detector blinding attacks	Quantum key distribution system	Conceiving novel QKD schemes
Makarov and Hjelme [31]	2005	Faked states attack	Quantum cryptosystems	Kak protocol
Wiechers *et al.,* [32]	2011	After-gate attack	Quantum cryptosystems	Performing higher privacy amplification
Tan *et al.,* [33]	2021	Wavelength attack	continuous-variable quantum key distribution	Conceiving novel QKD schemes
Jain *et al.,* [34]	2014	Trojan-horse attack	quantum key distribution System	Avoid intuitive measurements.

were presented in a paper that was subsequently published in the MIT Technology Review, demonstrated that a computer with 20 million qubits could decrypt a number with 2048 bits in around eight hours. This data indicates that if more advancements of a similar kind can be achieved in the future, we will continue to make ground and will be able to move the timeline forward.

When discussing the danger posed by quantum encryption, it is important to point out that the perishability of sensitive data is not the primary worry. The susceptibility of information that has to maintain its secret far into the future is the bigger danger. This includes information that falls under national security-level categories, financial data, privacy act data, and so on. Because dishonest individuals are already stealing this information while they wait for a quantum computer that is capable of breaking the encryption, these are the secrets that need to be secured with encryption that is quantum-proof right now.

Encryption is still an important part of how society works, but it also comes with risks and worries. If commercial quantum computers got powerful enough to break public-key encryption, it would be a big problem for a country's national security and the privacy of its financial, medical, and other kinds of data.

Many different parts of cryptography depend on computational complexity arguments, which are sometimes called math [36]. The fact that no one has been able to find a technique to break an algorithm within an acceptable period for it to be a problem is what gives an algorithm its reputation for being secure. Most of the time, the parameters of the algorithms used in cryptography can be changed to give different levels of security. For example, the width of an RSA key can be anywhere from 32 bits to 4096 bits, depending on how secure it needs to be. In the past, a key length of 512 bits for RSA was believed to provide an appropriate level of security. But as computer power has grown and cyberattacks have become more complicated, society has responded by gradually making keys longer to protect itself. However, the longer the keys are, the less useful an algorithm becomes; there is a balance to be struck between the use of the method and its level of security [36].

Recent data breaches have shown that most businesses keep data for longer than is required by law or than it is useful. The danger here is that data that is taken today does not necessarily need to be decrypted today for it to have value. Thefts of intellectual property, financial data, healthcare data, and other sensitive information might have repercussions far beyond the next decade. And those who commit cybercrime are aware of this. It is possible that a large-scale quantum computer could make it possible to decrypt most of the common security protocols and all of the traffic that has already been recorded. This would threaten the growth of our economy, our national security, and a big part of our everyday lives.

V. Quantum approaches to cybersecurity Concerns

There are a lot of mysteries in the field of quantum computing, and researchers are still working hard to figure them out. Despite this, there is one thing that can be said with absolute certainty about the effect that quantum computing will have on cybersecurity: it will pose a risk to both cybersecurity and the encryption methods that we use now. To lessen the impact of this risk, we have to adjust the way we maintain the safety of our data and get started doing it right now. We need to handle the quantum threat in the same manner that we handle other security weaknesses. This means putting in place a defense-in-depth strategy, which is a plan with several levels of protection that are quantum-safe. Table II shows the existing quantum-based approaches in the cybersecurity field. The need for cryptographic agility is something that forward-thinking security companies are aware of, and as a result, they are searching for crypto-diverse solutions such as those provided by Quantum exchange to make their encryption quantum-safe right now and quantum-ready for the threats of the future [35].

It is essential to keep in mind that quantum technologies have been around since the beginning of time. MRI machines, LED lights, and even the GPS clocks in cars are all examples

of technologies made possible by quantum physics. Even though the exact year that quantum computers will be able to do useful work is unknown (current projections put the year at 2030), the first step is to recognize that they will have an effect on the cryptography used today and that the solutions that are in place for cybersecurity will largely be insufficient. This is the time to think about such a threat [37].

The following constraints are a seismic shift for cryptography, which means we need to rethink our information security strategy in depth. Cryptographers are already looking into different ways to protect against the dangers of quantum computing, which they see as a worthwhile task in and of itself [38].

Quantum Poverty Every company and every member of the community has to take immediate action to lower the danger. When quantum technology becomes more common, a strategy like the global technology councils that have been set up to control artificial intelligence may be needed to keep an eye on all of the principles and models of global governance. This scenario is possible because global technology councils have been formed to control AI. You might add items to a list of principles, such as supporting the ethical use of quantum resources and making sure that quantum infrastructure is not used to break standard encryption. These are both examples of things that may be included. You could also make sure that everyone has the same access to quantum technologies to stop "quantum poverty," which happens when some people can't use these technologies because they aren't available to them.

Increasing Quantum Literacy It will be very vital to take the step of increasing "quantum literacy" across the ecosystem, both at the level of business leadership and at the level of policy leadership. Leaders need to know what is meant by "quantum technology," what its different parts are, when and how it might become available, what risks come with it and how they affect organizations, and what needs to be protected because of that. This education and training are necessary because they are necessary. This is because there is a need for educational and vocational opportunities. Enterprise leaders will be among the first to have to figure out how big the quantum risk is for their business and decide when and how to act. In addition to this, a risk assessment has to be done to determine which industries, if any, need to collaborate to address the problem. When it is unclear who is responsible for this change, this is the single most critical thing that you should do.

Advanced Cryptography The approach to post-quantum cryptography that is the simplest to understand is centered on the development of algorithms that are challenging even for quantum computers to decrypt. This method is useful because it works with regular computers. One possible solution would be to give people incentives to use encryption that can't be broken by quantum computers. However, to protect the global ecosystem, laws and rules would also need to be put in place. Standards like the NIST's post-quantum cryptography challenge can make it clear what practices each organization should use. Also, by making sure that these and other similar standards can be used internationally, we can take a big step toward making them more widely used around the world.

Lattice-based Algorithms Lattice-based algorithms are a different way to do cryptography that can be used instead of traditional methods. This is yet another possibility. The methods, which are usually only talked about in scientific circles, were made to be safe and did not depend on any assumptions about how the processing power would be used in the end. Companies like Google have begun testing post-quantum cryptography methods that make use of lattice-based algorithms. These methods are also being worked on by the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and other government agencies. The National Institute of Standards and Technology (NIST) has been working on establishing tools to analyze these new algorithms, and it anticipates publishing its results between the years 2022 and 2024 [10].

Integrity Assurance In both the staff onboarding process and the customer onboarding process, cloud identity providers and cybersecurity vendors play an important role. If the mission is to be successful, both authentication and communication must be kept honest. Key strategies that should be in any playbook are testing encryption methods all the time, making sure that key transfers are safe, and slowly adopting new cryptographic algorithms as they come out. Also, businesses have a duty to invest in resources that protect both the encrypted conversations they store and the user data. These regions cannot afford to remain susceptible to the computational power of the future. Okta [10] puts a lot of importance on keeping the authentication and multi-factor authentication processes private so that they can do what it's supposed to do, which is connect everything. While we will continue to make sure that the authentications used today are tried and true, we will also keep an eye out for what the future has in store for us.

Post-quantum Security The term "post-quantum security" is often used interchangeably with "quantum-safe security." Let's begin with the worst possible outcome, just as we would if we were modeling a security issue [56]. Let's say that the side that you can trust uses a classical computer, and the side that you can't trust uses a quantum computer. In the old world, we would want to build a security system that could not be broken, not even by an opponent who could use quantum computing. The term "post-quantum security" refers to the state of being successful despite adverse conditions. This is one subject that is receiving a lot of attention from researchers these days. Let's have a look at the steps that need to be taken to reach such a post-quantum security paradigm.

Post-quantum Algorithmic System Two different strategies are being looked into right now to protect society from the risks that quantum computing could pose. The first category consists of post-quantum algorithmic systems. This cryptographic method can be used on today's computers, and it is anticipated that it will be resistant to quantum assaults. Another complementary approach that is now being worked on is based on using quantum technology. Even if there is a possibility that the improper application of quantum technology might

TABLE II: **Existing Quantum-based Approaches for Cybersecurity**

Author / Ref	Year	Security Type	Key Contribution	Findings
carames *et al.,* [39]	2020	Blockchain, Distributed Ledger, Cryptography	Quantum-resistant blockchain cryptography.	Introduces encryption for the blockchain that is immune to assaults from quantum computers.
Althobaiti and Dohler [40]	2020	Security for post-quantum IoT	Post-Quantum Internet of Things cybersecurity issues.	Security concerns relating to the Internet of Things that stem from the post-quantum era.
Kuznetsov *et al.,* [41]	2020	Cryptography and Digital Signature	Error-correcting post-quantum digital signatures	Schemes for post-quantum digital signatures that are based on the use of error-correcting codes
Al-darwbi*et al.,* [42]	2021	Safety key Management.	Scalable quantum-safe key management	A key management system that is both scalable and quantum-safe.
Dixit *et al.,* [43]	2022	quantum annealing-based cybersecurity	Quantum annealing-based restricted Boltzmann machine cybersecurity.	With the help of a limited Boltzmann machine, quantum annealing-based cybersecurity may be achieved.
Kilber*et al.,* [13]	2021	quantum threats	Cybersecurity for quantum computing considering quantum concerns.	Protection of information for quantum computing focuses on quantum risks and vulnerabilities.
Libicki and Gompert [44]	2021	Communication Security.	Post-pandemic cybersecurity via quantum communication.	The use of quantum communication in the post-pandemic security sector.
Yan *et al.,* [45]	2021	Security key distribution	MDI-QKD-based microgrid control architecture.	Quantum key distribution (MDI-QKD) is the foundation of the microgrid control architecture being developed.
Zhou *et al.,* [46]	2018	Quantum key distribution (QKD)	Future internet security with quantum cryptography	Quantum cryptography is essential for the continued safety of the internet in the future.
Suryotrisongko,and Musashi [47]	2022	DGA botnet detection	Cybersecurity hybrid quantum-classical deep learning model.	Model for deep learning that combines quantum and conventional techniques, with application to cybersecurity.
Abd El-Latif*et al.,* [48]	2021	Authentication for cybersecurity	Quantum walk-inspired authentication and encryption protocol (QIQW)	Protocol for authentication and encryption based on quantum walks, which were inspired by quantum mechanics (QIQW).
Mosca [49]	2018	post-quantum cybersecurity	Quantum-key distribution (QKD) and cryptography	Quantum cryptography, as well as the distribution of quantum keys.
Dixit *et al.,* [50]	2021	Cybersecurity and Bar-and-stripes (BAS)	Quantum computing with restricted Boltzmann machine (RBM)	Computing on the quantum level by using a Boltzmann machine with certain restrictions (RBM).
Edwards*et al.,* [51]	2021	Encryption-based key exchange	CoreVUE post-quantum security bypasses PKI.	CoreVUE, a post-quantum security protocol, is able to circumvent PKI.
Albataineh and Nijim [52]	2021	cybersecurtiy in education	Quantum computation-based cybersecurity education	Quantum computing in the context of cybersecurity education and training programs.
Neukart*et al.,* [53]	2017	Quantum Traffic Flow	Quantum annealer traffic optimization.	Optimization of the flow of traffic via a quantum annealer.
Ko and Jung [54]	2021	Encryption and Decryption	Quantum computing to encrypt/decrypt cybersecurity data using Advanced Encryption Standard (AES).	Encryption and decryption of sensitive data in the field of cybersecurity using an algorithm based on the AES and quantum computing.
Hassija *et al.,* [55]	2020	Random key generation	Cybersecurity quantum random number generators	Random number generators based on quantum mechanics for use in cybersecurity.

compromise our capacity to encrypt information and securely communicate it, there is now equipment on the market that can reduce these dangers.

Post-quantum Cryptography (PQC) One possible answer is for companies and other organizations to begin researching post-quantum cryptography (PQC) algorithms and to replace their existing ones with new ones that are resistant to quantum computing. The National Institute of Standards and Technology (NIST) has found the first four encryption algorithms that it thinks would be able to stand up to quantum computing. Businesses should look into the safety of post-quantum candidates and switch to using these algorithms to make sure that their data stays safe. Start by figuring out which alternatives are the most likely to work, and then plan your transition while keeping in mind that PQC solutions are not yet fully developed.

Advance Quantum key distribution (QKD) Quantum key distribution (QKD) is an additional possibility. This results in the creation of a common, shared secret between the users, which can then be used to create secure communications that may be sent over standard channels. To get forward secrecy, however, QKD needs specialized equipment, such as the best possible optical fiber infrastructure. It is a way to make sure that stolen session keys can't be used to do bad things. In addition, companies need to think about revising their procurement procedures and making it a requirement that any future technology purchases need to have cryptographic flexibility. This means being able to add and switch to newer algorithms that are more secure when they become available.

Next-Generation Quantum Secuirty Realistically, quantum security shouldn't be seen as a substitute for the measures that are already in place; rather, it should be considered as an extra kind of security that will need to be handled in conjunction with the infrastructure that is already in place. Conventional and post-quantum security measures will need to be implemented, managed, and maintained on an organization's systems. These issues will need to be taken into consideration by the organization. The security industry is now dealing with a variety of structural issues brought on by the technologies of the next generation. Even while the improper use of quantum technology might put a damper on our capacity to encrypt data and safely communicate it with others, there

is already equipment on the market that can offset the threats posed by quantum computing.

Information security rather than mathematical security makes the one-time pad the only quantum-safe cryptography [57]. Technically, QKD is safe because any attempt to get the keys for mathematical decryption will destroy the keys, making it impossible to use them to decrypt the message. QKD has some problems that make it hard to use in general, but modern technology may be able to make useful one-time pads. OTP needs keys longer than the message being encrypted, making it unsuitable for the internet. However, some firms are researching the prospects of new technology [58].

Qrypt began with the idea that encryption key transmission poses a quantum hazard. Avoiding critical communication eliminates the danger. It devised a method to generate identical quantum random numbers at the source and destination. Quantum physics generates really random numbers. These numbers may produce identical keys without internet transmission. Since the numbers may be generated and saved until use, the procedure can be chained to give an authentic OTP for the keys without sending them over the internet. This approach yields quantum-secure solutions [58].

Incrypteon Shannon's information theories were used by the British company in the one-time pad. The science is mind-numbing yet based on Shannon's 1949 Communication Theory of Secrecy Systems Equivocation. Encryption claims that statistics and probability define complete secrecy. A ciphertext keeps everything completely secret if the attacker knows the same thing about the message's contents before and after inspecting it with unlimited resources. Encryption ensures that conditional entropy never equals 0, therefore establishing "perfect secrecy" through its unique software and "perpetual equivocation." It's accessible now and automatically quantum secure [58].

Rixon Another startup, Rixon, is participating. It protects web-based enterprises' PII, but its concepts may be used elsewhere. Plaintext is tokenized in the cloud and never stored. The cloud tokenization engine stores just the tokenization path for each tokenized character, not the plaintext (for the purpose of comparison, this tokenization route is equivalent to the cryptographic key but is random for each character). The OTP's "key" matches the message's length. Rixon tokenizes personally identifiable information, but it could also protect intellectual property and business strategies [58].

VI. Future of Quantum Computing

The development of countermeasure technologies against future cyberattacks is not the only factor that will determine how safe the future will be. We need to work together on a global scale to set up the proper governance that will encourage the development and use of quantum security technologies in the global ecosystem, as shown in Fig. 4. It's becoming more and more important for people to be able to communicate safely and do math well at the same time. Both the computer and the internet have had a truly transformative impact on the society we live in.

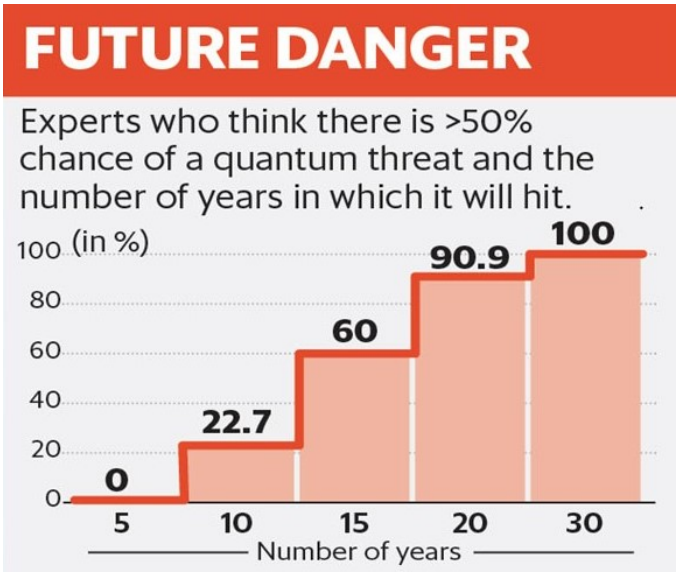

Fig. 4: The chronology of the quantum threat [14].

In the next five to ten years, there will be an explosion of new possible scenarios as quantum technologies become more integrated into the current computing and communication infrastructure. In the future, networks will almost certainly have both classical and quantum devices and links [59]. Some of these classical and quantum devices and links are likely to be lying. Different parts of these future networks will have different levels of complexity, from simple routers to servers that can run universal quantum algorithms [60]. For such a complex network of classical and quantum communication to work, it needs to be built on a strong and innovative foundation that, despite being new, is flexible enough to handle the complexity of real-world implementations and new applications.

Post-quantum security paves the way for our classical internet to stay safe in that era [61]. On the other hand, quantum-enhanced security wants to take advantage of the development of quantum communication to achieve performance levels that can't be reached with classical communication. This is different from post-quantum security, which makes it possible for our old communications to still be safe in the future. Quantum-enabled security gives users the infrastructure they need to be sure that the quantum cloud's new, unmatched computing power meets the right standards for accuracy, reliability, and privacy. This will be accomplished through the utilization of the quantum cloud [62].

Most government organizations and private businesses will need to take three main steps to prepare their digital infrastructure for quantum-resilient cybersecurity [63]. To start, the current encryption, which can be broken by quantum attacks, should be looked at and written down. Create a strategy to implement quantum-safe cryptography in your network wherever it is necessary, including servers, edge devices, and Internet of Things devices, and Conduct tests in your information technology infrastructure using a system that is

quantum-safe and cryptographically agile [64]. When working with an experienced consultant or service provider, it may not take long to choose the right cryptographic algorithms. Quantum-safe security solutions, on the other hand, will take more time to set up because of the size and complexity of your organization's network.

In the traditional form of computing, each bit represents either a one or a zero. However, in quantum computing, a quantum bit, also known as a qubit, can hold both the value one and zero at the same time. This paves the way for a whole new set of possibilities regarding the capabilities of computers. Since quantum computers are able to test out several potential answers all at once, they are able to solve problems far more quickly than traditional computers. They are also not restricted by the same limits that traditional computers are, which means that they can tackle issues that are now difficult to address. Because of this, quantum computing is a great option for giving artificial intelligence (AI) its power. AI systems need large amounts of computer power in order to handle the immense volumes of data they analyze [65]. Quantum computing has the ability to fulfill this need for power and open the door for AI to realize its full potential.

VII. Conclusions

The emergence of quantum computing poses a significant threat to cybersecurity. It has the potential to break many of the encryption methods that are currently used to protect sensitive information. As quantum computers become more powerful and widespread, it will be necessary to develop new encryption methods that are resistant to quantum attacks. Fortunately, efforts are already underway to develop quantum-resistant cryptography, including lattice-based cryptography and code-based cryptography. These new encryption methods are designed to be resistant to attacks from both classical and quantum computers, making them a viable solution for securing sensitive information in the quantum computing paradigm. It is also important to note that cybersecurity is a constantly evolving field, and as quantum computing continues to develop, so too will the strategies and tools used to defend against cyber threats. By staying informed and proactive, individuals and organizations can help ensure the security of their digital assets in the face of this new paradigm.

Conflicts of interest: The authors have no conflicts of interest to declare that are relevant to the content of this article.

Data Availability Statement: This manuscript has no associated data.

References

[1] P. Wallden and E. Kashefi, "Cyber security in the quantum era," *Communications of the ACM*, vol. 62, no. 4, pp. 120–120, 2019.

[2] K. Keplinger, "Is quantum computing becoming relevant to cybersecurity?" *Network Security*, vol. 2018, no. 9, pp. 16–19, 2018.

[3] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, 2012.

[4] J. WALKER, "Quantum computing is coming: How will it impact cybersecurity?" https://www.entrepreneur.com/en-au/technology/quantum-computing-is-coming-how-will-it-impact/439060, 2022, [Online; Accessed on Jan. 12, 2023].

[5] L. Axon, S. Creese, J. Saunders, and W. Dixon, "Why we need to solve our quantum security challenges," https://www.weforum.org/agenda/2020/06/quantum-computers-security-challenges/, 2020, [Online; Accessed on Jan. 27, 2023].

[6] A. Ali, "A pragmatic analysis of pre-and post-quantum cyber security scenarios," in *2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)*. IEEE, 2021, pp. 686–692.

[7] V. Bindu, "Cyber security analysis for quantum computing," *Journal of IoT in social, mobile, analytics and cloud*, vol. 4, no. 2, pp. 133–142, 2022.

[8] C. Kim, K. D. Park, and J.-K. Rhee, "Quantum error mitigation with artificial neural network," *IEEE Access*, vol. 8, pp. 188 853–188 860, 2020.

[9] V. Sharma and H. B. A. FAA, "Rethinking cybersecurity for a quantum world," https://www.science.org.au/curious/policy-features/rethinking-cybersecurity-quantum-world, 2020, [Online; Accessed on Jan. 30, 2023].

[10] S. Sham, "The impact of quantum computing on cybersecurity," https://www.okta.com/blog/2019/07/the-impact-of-quantum-computing-on-cybersecurity/, 2019, [Online; Accessed on Feb. 01, 2023].

[11] M. Ohzeki, "Breaking limitation of quantum annealer in solving optimization problems under constraints," *Scientific reports*, vol. 10, no. 1, pp. 1–12, 2020.

[12] NIST, "Nist announces first four quantum-resistant cryptographic algorithms," https://www.entrepreneur.com/en-au/technology/quantum-computing-is-coming-how-will-it-impact/439060, 2022, [Online; Accessed on Jan. 12, 2023].

[13] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," *arXiv preprint arXiv:2110.14701*, 2021.

[14] P. Mukhopadhyay, "A cyber security perspective on quantum computing," https://www.opensourceforu.com/2020/04/a-cyber-security-perspective-on-quantum-computing/, 2020, [Online; Accessed on Jan. 16, 2023].

[15] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-key-distribution-based microgrid control for cybersecurity enhancement," *IEEE Transactions on Industry Applications*, vol. 58, no. 3, pp. 3076–3086, 2022.

[16] X. Liu, A. Angone, R. Shaydulin, I. Safro, Y. Alexeev, and L. Cincio, "Layer vqe: A variational approach for combinatorial optimization on noisy quantum computers," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–20, 2022.

[17] J. Kaur and K. Ramkumar, "The recent trends in cyber security: A review," *Journal of King Saud University-Computer and Information Sciences*, 2021.

[18] R. Hamerly, T. Inagaki, P. L. McMahon, D. Venturelli, A. Marandi, T. Onodera, E. Ng, C. Langrock, K. Inaba, T. Honjo *et al.*, "Experimental investigation of performance differences between coherent ising machines and a quantum annealer," *Science advances*, vol. 5, no. 5, p. eaau0823, 2019.

[19] D. M. Turner, "When will quantum computing arrive and how will it impact cybersecurity?" https://www.cryptomathic.com/news-events/blog/when-will-quantum-computing-arrive-and-how-will-it-impact-cybersecurity, 2022, [Online; Accessed on Feb. 01, 2023].

[20] R. Meraz and L. Vahala, "Application of quantum cryptography to cybersecurity and critical infrastructures in space communications," *OUR Journal: ODU Undergraduate Research Journal*, vol. 7, no. 1, p. 5, 2020.

[21] P. Ducklin, "Us passes the quantum computing cybersecurity preparedness act – and why not?" https://nakedsecurity.sophos.com/2022/12/29/us-passes-the-quantum-computing-cybersecurity-preparedness-act-and-why-not/, 2022, [Online; Accessed on Feb. 03, 2023].

[22] G. Mogos, "Intercept-resend attack on quantum key distribution protocols with two, three and four-state systems: Comparative analysis," in *2015 2nd International Conference on Information Science and Security (ICISS)*, 2015, pp. 1–4.

[23] A. Gaidash, V. Egorov, and A. Gleim, "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices," in *Journal of Physics: Conference Series*, vol. 735, no. 1. IOP Publishing, 2016, p. 012072.

[24] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[25] C. Zhou, W. Bao, and X. Fu, "Information-disturbance tradeoff of individual attack against bbm92 protocol," in *2010 International Conference on Communications and Mobile Computing*, vol. 1, 2010, pp. 31–34.

[26] T. Iwakoshi, "Security evaluation of y00 protocol based on time-translational symmetry under quantum collective known-plaintext attacks," *IEEE Access*, vol. 9, pp. 31 608–31 617, 2021.

[27] A. Ferenczi, P. Grangier, and F. Grosshans, "Calibration attack and defense in continuous variable quantum key distribution," in *2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*, 2007, pp. 1–1.

[28] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Eavesdropping of two-way coherent-state quantum cryptography via gaussian quantum cloning machines," in *2009 Third International Conference on Quantum, Nano and Micro Technologies*, 2009, pp. 38–41.

[29] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080*, 2005.

[30] C. Navas-Merlo and J. C. Garcia-Escartin, "Detector blinding attacks on counterfactual quantum key distribution," *Quantum Information Processing*, vol. 20, no. 6, p. 196, 2021.

[31] V. Makarov* and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

[32] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, no. 1, p. 013043, 2011.

[33] X. Tan, Y. Guo, L. Zhang, J. Huang, J. Shi, and D. Huang, "Wavelength attack on atmospheric continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 103, p. 012417, Jan 2021. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.103.012417

[34] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of trojan-horse attacks on practical quantum key distribution systems," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 168–177, 2014.

[35] Quantumexchange, "What is the impact of quantum computing on cybersecurity?" https://quantumxc.com/blog/quantum-computing-impact-on-cybersecurity/, [Online; Accessed on Feb. 02, 2023].

[36] L. Kleinman, "The quantum effect on cybersecurity," https://www.forbes.com/sites/forbestechcouncil/2023/02/09/the-quantum-effect-on-cybersecurity/amp/, 2023, [Online; Accessed on Feb. 12, 2023].

[37] F. Raheman, "The future of cybersecurity in the age of quantum computers," *Future Internet*, vol. 14, no. 11, p. 335, 2022.

[38] F. Hu, L. Lamata, M. Sanz, X. Chen, X. Chen, C. Wang, and E. Solano, "Quantum computing cryptography: Finding cryptographic boolean functions with quantum annealing by a 2000 qubit d-wave quantum computer," *Physics Letters A*, vol. 384, no. 10, p. 126214, 2020.

[39] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[40] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157 356–157 381, 2020.

[41] A. Kuznetsov, A. Kiian, V. Babenko, I. Perevozova, I. Chepurko, and O. Smirnov, "New approach to the implementation of post-quantum digital signature scheme," in *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020, pp. 166–171.

[42] M. Y. Al-darwbi, A. A. Ghorbani, and A. H. Lashkari, "Keyshield: A scalable and quantum-safe key management scheme," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 87–101, 2021.

[43] V. Dixit, R. Selvarajan, T. Aldwairi, Y. Koshka, M. A. Novotny, T. S. Humble, M. A. Alam, and S. Kais, "Training a quantum annealing based restricted boltzmann machine on cybersecurity data," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 3, pp. 417–428, 2022.

[44] M. C. Libicki and D. Gompert, "Quantum communication for post-pandemic cybersecurity," in *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, pp. 371–386.

[45] R. Yan, J. Dai, Y. Wang, Y. Xu, and A. Qun Liu, "Quantum-key-distribution based microgrid control for cybersecurity enhancement," in *2021 IEEE Industry Applications Society Annual Meeting (IAS)*, 2021, pp. 1–7.

[46] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," *Security and Communication Networks*, vol. 2018, pp. 1–7, 2018.

[47] H. Suryotrisongko and Y. Musashi, "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet dga detection," *Procedia Computer Science*, vol. 197, pp. 223–229, 2022.

[48] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in iot-based smart cities," *Information Processing & Management*, vol. 58, no. 4, p. 102549, 2021.

[49] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[50] V. Dixit, Y. Koshka, T. Aldwairi, and M. Novotny, "Comparison of quantum and classical methods for labels and patterns in restricted boltzmann machines," in *Journal of Physics: Conference Series*, vol. 2122, no. 1. IOP Publishing, 2021, p. 012007.

[51] N. Edwards, J. B. Haynes, and S. B. Kiser, "Post-quantum security: Corevue breaks through pki a look at an emerging technology in cybersecurity," *Journal of Strategic Innovation and Sustainability*, vol. 16, no. 1, pp. 136–138, 2021.

[52] H. Albataineh and M. Nijim, "Enhancing the cybersecurity education curricula through quantum computation," in *Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20*. Springer, 2021, pp. 223–231.

[53] F. Neukart, G. Compostella, C. Seidel, D. Von Dollen, S. Yarkoni, and B. Parney, "Traffic flow optimization using a quantum annealer," *Frontiers in ICT*, vol. 4, p. 29, 2017.

[54] K.-K. Ko and E.-S. Jung, "Development of cybersecurity technology and algorithm based on quantum computing," *Applied Sciences*, vol. 11, no. 19, p. 9085, 2021.

[55] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, and M. Guizani, "Present landscape of quantum computing," *IET Quantum Communication*, vol. 1, no. 2, pp. 42–48, 2020.

[56] H. Alyami, M. Nadeem, W. Alosaimi, A. Alharbi, R. Kumar, B. K. Gupta, A. Agrawal, and R. A. Khan, "Analyzing the data of software security life-span: Quantum computing era." *Intelligent Automation & Soft Computing*, vol. 31, no. 2, 2022.

[57] M. J. H. Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*. IEEE, 2022, pp. 1–8.

[58] K. Townsend, "Cyber insights 2023 — quantum computing and the coming cryptopocalypse," https://www.securityweek.com/cyber-insights-2023-quantum-computing-and-the-coming-cryptopocalypse/amp/, 2023, [Online; Accessed on Feb. 8, 2023].

[59] F. B. Maciejewski, Z. Zimborás, and M. Oszmaniec, "Mitigation of readout noise in near-term quantum devices by classical post-processing based on detector tomography," *Quantum*, vol. 4, p. 257, 2020.

[60] R. Ayanzadeh, M. Halem, and T. Finin, "Reinforcement quantum annealing: A hybrid quantum learning automata," *Scientific reports*, vol. 10, no. 1, pp. 1–11, 2020.

[61] S. S. Tannu and M. K. Qureshi, "Mitigating measurement errors in quantum computers by exploiting state-dependent bias," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, 2019, pp. 279–290.

[62] S. Heng, D. Kim, T. Kim, and Y. Han, "How to solve combinatorial optimization problems using real quantum machines: A recent survey," *IEEE Access*, vol. 10, pp. 120 106–120 121, 2022.

[63] S. Sanzeri, "What the quantum computing cybersecurity preparedness act means for national security," https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-secu amp/, 2023, [Online; Accessed on Feb. 7, 2023].

[64] K. K. Rangan, J. Abou Halloun, H. Oyama, S. Cherney, I. A. Assoumani, N. Jairazbhoy, H. Durand, and S. K. Ng, "Quantum computing and resilient design perspectives for cybersecurity of feedback systems," *IFAC-PapersOnLine*, vol. 55, no. 7, pp. 703–708, 2022.

[65] D. Edwards and D. B. Rawat, "Quantum adversarial machine learning: Status, challenges and perspectives," in *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 2020, pp. 128–133.