Sri Lanka Institute of Information Technology

QUANTUM COMPUTING AND ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

IE2022 – Introduction to Cyber Security -

Student Name	Student ID
Pemarathna I.R.C	IT21170416

Table of Contents

Abstract

This study builds on some of the quantum computing properties and artificial intelligence embedded computer system benefits for cyber security. Also, explain what quantum computers and quantum physics are. what is quantum cryptography and how to utilize it safely, explain artificial intelligence, show the relationship between AI and quantum computing, install cyber security, and mold cyber security using The quantum risk Compare the risks of quantum computing and AI, as well as how to use them against cyber criminals. how to improve cyber security with encryption and quantum computing Existence of quantum computing, appraisal, and future of security quantum computing and AI.

Introduction

What is a quantum?

The smallest discrete unit of a phenomena is referred to as a quantum (plural: quanta). A photon is a quantum of light, while an electron is a quantum of electricity. Quantum is derived from Latin and means "quantity" or "how much?" If anything can be quantified, it can be measured. [1]

https://www.techtarget.com/whatis/definition/quantum

What is quantum in physics?

Max Planck first used the term "quantum" in physics in 1901. He was attempting to explain black-body radiation as well as how heated items changed color. He proposed that the energy was released in discrete packets, or bundles, as opposed to being assumed to be released in a continuous wave. These were referred to as energy quanta. As a result, he discovered the Planck constant, a basic universal quantity. [2]

what is the a qubit?

The fundamental piece of information in quantum computing is a qubit. [3]

https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing/#introduction

What are Quantum computers?

They use quantum physics, which is most visible in the behavior of atoms, electrons, photons, and other tiny particles, to process information differently than computers. Quantum computers do multiple simultaneous calculations on bits that can be in a quantum "superposition" of states, not simply one or zero. Controlling qubits can enhance computer efficiency and power exponentially. [4]

https://evolutionq.com/quantum-safe-cyber-security-faq.html

What is quantum computing?

While both conventional and quantum computers aim to find solutions, they do so in fundamentally different ways by manipulating data. This section introduces two fundamental concepts of quantum physics, superposition, and

entanglement, which are essential to the understanding of what makes quantum computers special. [5]
https://www.ncbi.nlm.nih.gov/books/NBK538701/#sec_000009

What quantum cryptography is used?

In comparison to regular cryptography, quantum cryptography allows users to communicate more securely. After the keys have been shared between the people involved, there is little risk that a hostile actor may decode the material without the key. The intended outcome changes if the key is detected as it is being produced, informing both the sender and the recipient. [6]

https://www.techtarget.com/searchsecurity/definition/quantum-cryptography

What exactly is "quantum-safe cryptography?"

It is a method of keeping information safe in the face of the impending arrival of new quantum computers, which will be strong enough to breach the methods we currently use to preserve the privacy and authenticity of critical data. [7]

https://evolutionq.com/quantum-safe-cyber-security-faq.html

What is Artificial Intelligence (AI)?

Artificial intelligence (AI) is a combination of technologies that allows computers to perform a wide range of sophisticated operations, such as seeing, understanding, and translating spoken and written language, analyzing data, making suggestions, and so on. [8]

https://cloud.google.com/learn/what-is-artificial-intelligence

What is the relationship between Artificial Intelligence and quantum computing?

possibly having various effects on AI. One example is that quantum computers could be able to do some operations more quickly than traditional computers, which might lead to quicker decision-making (e.g., to inform hyper speed parameter use cases). A broader reach might also offer AI systems access to more data, perhaps enabling them to learn more effectively from the insights, as quantum computers can store and analyze more data than conventional computers. [9]

https://pub.towardsai.net/the-future-of-ai-is-quantum-computing-10-of-the-most-important-use-cases-3a4b50c58f3e

Artificial Intelligence and Quantum computing in cybersecurity

AI increases the rate of danger detection while reducing mistakes.
Quantum computing will enable quantum key distribution (QKD) by distributing cryptographic codes among users while assuring perfect security and reporting unauthorized intrusions.
To address the threat posed by quantum computing in revealing encryptions, research is being conducted to build quantum-safe encryption.
AI may be used to monitor network security and data centers in order to detect anomalies and respond to vulnerabilities by understanding their causes.
Quantum machine learning can accelerate the development of algorithms that improve cybersecurity safeguards.
Although quantum computing is viewed as a danger to cybersecurity, if properly capitalized, it might be a catalyst for providing greater security with disruptors such as AI. [10]

https://www.analyticsinsight.net/ai-and-quantum-computing-in-securing-the-cyberspace/

How Quantum Computing and Machine Learning are Shaping Cybersecurity

Faster corporate transformation, new multi-channel experiences, and individuals working from home are all contributing factors to the evolution of cybersecurity, which is currently a top concern. Organizations are looking to technologies like quantum computing and machine learning (ML) to stay ahead of the changing threat environment as new security concerns emerge. [11]

How Quantum Computing and Machine Learning are Shaping Cybersecurity (simplilearn.com)

Quantum danger

The capacity of quantum computers to swiftly and easily crack present cryptography might pose the greatest threat to the globe. [12]

Is quantum computing more dangerous than AI? - Tech Monitor

Risks of AI?

Invasion of Data Privacy , Self-Crashing Vehicles, Loss of Skills , Discrimination , Autonomous Weapons ,Social Manipulation [13]

Top 6 Potential Dangers of AI Technology You Never Knew | CellularNews (robots.net)

Is quantum computing more dangerous than AI?

A famous professor has cautioned that if enough regulation is not put in place around quantum computing, it might be "more hazardous than artificial intelligence." However, with quantum devices now making their way out of laboratories and into the real world, it may be too late to adequately govern their use. [14]

Is quantum computing more dangerous than AI? - Tech Monitor

AI and Quantum Computers Are Our Best Weapons Against Cyber Criminals

- WEAPONS OF CYBER WARFARE

  Cybersecurity has emerged as a critical topic in national and worldwide debates.
  Cyber assaults no longer affect solely email firms and individuals that refuse to upgrade their technology. Cybercrime has now had a significant influence on both the U.S.
  major political parties, as well as practically any organization, including hospitals, should have some reservations about the likelihood of an assault via a computer network In their efforts to combat cybercrime, large corporations such as IBM are resorting to two of the most powerful technologies in the world – artificial intelligence (AI) and quantum computing [15]

AI and Quantum Computers Are Our Best Weapons Against Cyber Criminals (futurism.com)

- TIME FOR FASTER FIGHTERS

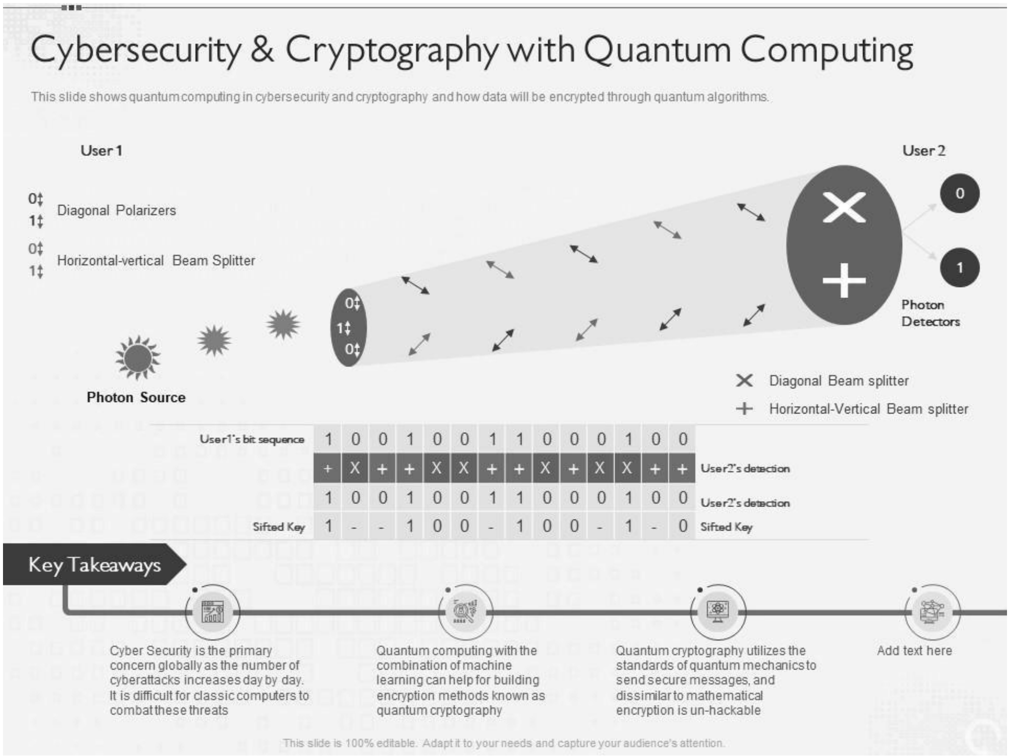
  IBM **Watson** is artificial intelligence for business. Watson assists firms in forecasting future events, automating difficult procedures, and optimizing staff time.
  https://www.ibm.com/watson/about

  Watson is around 60 times quicker than its human equivalents, and speed is critical in cyber defense. However, even Watson's amazing rates pale in comparison to those achievable with quantum computers.
  "We prefer to think of it as a needle in a haystack." "In the interview, Driver stated. "A machine can be carefully designed to look for a needle in a haystack, but it must still check beneath each bit of hay. Quantum computing means I'll examine beneath every piece of hay at the same time and discover the needle right away." [16]

  https://futurism.com/ai-and-quantum-computers-are-our-best-weapons-against-cyber-criminals

How companies can use quantum technology and AI to improve cyber security

In today's digital environment, hackers are advancing in tandem with technical breakthroughs. Fortunately, engineers, mathematicians, and physicists are all working on novel ideas that leverage the evolution of traditional encryption approaches. New gadgets are employing quantum physics concepts and sophisticated and powerful algorithms for secure communication.



Cybersecurity & Cryptography with Quantum Computing

This slide shows quantum computing in cybersecurity and cryptography and how data will be encrypted through quantum algorithms.

User1's bit sequence	1	0	0	1	0	0	1	1	0	0	0	1	0	0	
	+	X	+	+	X	X	+	+	X	+	X	X	+	+	User2's detection
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	User2's detection
Sifted Key	1	-	-	1	0	0	-	1	0	0	-	1	-	0	Sifted Key

Key Takeaways

Cyber Security is the primary concern globally as the number of cyberattacks increases day by day. It is difficult for classic computers to combat these threats

Quantum computing with the combination of machine learning can help for building encryption methods known as quantum cryptography

Quantum cryptography utilizes the standards of quantum mechanics to send secure messages, and dissimilar to mathematical encryption is un-hackable

Add text here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Cybersecurity & Cryptography with Quantum Computing [17]

https://www.slideteam.net/quantum-computing-it-cybersecurity-and-cryptography-with-quantum-computing-ppt-skills.html

Exist Quantum Computers?

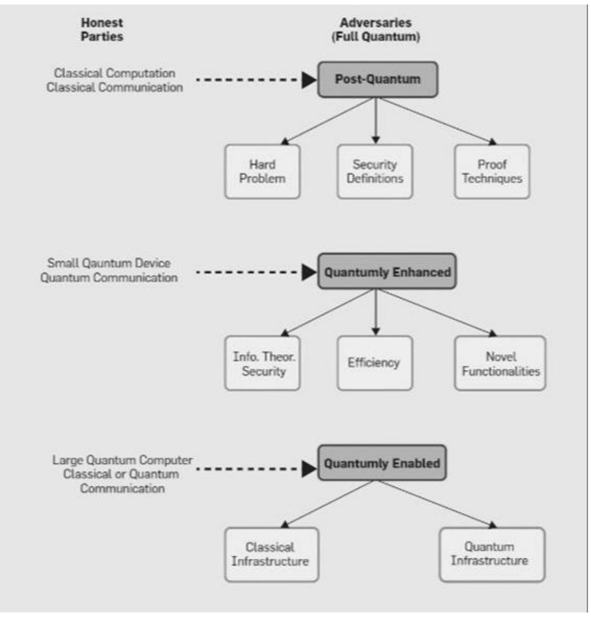
Yes, rudimentary, small-scale quantum computers have been created and shown effectively. These are now laboratory devices that are huge, costly, and difficult to operate, with extremely limited capabilities. They do, however, demonstrate that the basic physical concepts are correct.

The objective is to develop one that is large enough (in terms of qubit capacity) to outperform traditional computers at meaningful activities.

Many universities, firms, and government organizations across the world are racing to achieve this, employing a range of different experimental methodologies - some techniques may prove to be more practical than others, or have unique qualities that are advantageous for specific kinds of application.

Evolution

Artificial Intelligence and Quantum computing for cybersecurity evolution.



Schematic representation of the quantum cyber security research landscape. **[18]**

https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

A cyber attack is a digital attack coordinated by a state or government with the goal of harming computer systems and networks, performing acts of espionage, or destroying an adversary's or ally's key infrastructure. The greater reliance on technology in recent years has resulted in a substantial increase in the frequency of cyber warfare strikes. The Morris Worm was the first known hack, affecting around 6,000 machines. The cost of this hack ranged from $100,000 to millions of dollars (FBI, 2018). The Morris Worm only infected machines running a certain version of the Unix Operating System. The virus was blamed for significantly slowing computer functionality and emails, as well as destroying systems. Another illustration is the Stuxnet Worm, which had an impact on the Iranian nuclear program and was connected to the United States. Stuxnet was able to disable almost a thousand uranium enrichment centrifuges by concentrating its attack on Windows-based networks and computers. As a result, Iran's nuclear weapons development has slowed down. Stuxnet propagated so quickly that it was able to access and duplicate vital information. When a computer was used to access the USB drive that contained the Stuxnet Worm, the nuclear weapons facility's destruction process started (M. Holloway, 2015).

"Persistent and disruptive cyber operations will continue against the United States and our European allies, using elections as opportunities to undermine democracy, sow discord, and undermine our values," declared Daniel Coats, the current Director of National Intelligence, in a statement that highlighted how cyberwarfare poses a serious threat to national security. With the aim of undermining our democratic ideals and damaging our partnerships, some of these entities, especially Russia, are likely to launch ever more extreme cyberattacks. North Korea will continue to employ cyber operations to generate money, conduct attacks, and gather intelligence against the United States, while Iran will attempt to hack into American and allies' networks for espionage.

Both quantum computing and artificial intelligence have shown to have a significant influence on the development of warfare as we know it. Through the algorithms that run artificial intelligence systems, overly vast volumes of data may be gathered. The rules or patterns in the data used to create the algorithms can help artificial intelligence learn new skills. Although it has incredibly sophisticated capabilities, it is more than plausible that artificial intelligence may be utilized against us, leaving us vulnerable. To do several calculations at once, quantum computing can employ quantum mechanical engineering. The fastest and most effective computer ever created is a quantum computer. Theoretically, a single quantum computer would be more powerful than all of the world's supercomputers combined (J. Garamond , 2018). Theoretically, if a state completely mastered quantum computing, they would be able to attack networks, databases, and vital infrastructure systems with little to no resistance. Due to the extreme difficulty of guarding against artificial intelligence and quantum computing, these technologies have the potential to pose a grave threat to national security. **[19]**

https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/

AI and QC Cybersecurity

The advancement of AI and QC in contemporary combat has security ramifications. Digital advancements that have enabled our greatest strengths may also be our biggest dangers. As a country seeking to lead the world in the digital sphere, we must endeavor to secure our cyberspace and make it robust to future threats. While AI is being used as a weapon, to instruct robots, and to train drones and autonomous vehicles to inflict damage rather than good, it may be hidden and not viewed as a destructive instrument (Cetron, Davies, 2009). "We're still in the early days of attackers employing artificial intelligence themselves," said Nicole Eagan, CEO of cybersecurity firm Darktrace. And I believe that once the switch is flicked on, there will be no turning back, so we are quite concerned about the use of AI by attackers in various ways, including their ability to blend into the background of these networks." When it comes to QC and the race to construct a quantum computer, additional levels of protection are critical. To develop supremacy and defend itself in the process, the United States must begin to take safeguards to construct a security system, as well as expand technical training and collaboration with the private sector. The United States, according to NIST, "should begin immediately to prepare our information security systems to resist quantum computing." This includes everything from safeguarding the computers that residents use every day to safeguarding the key infrastructure on which we rely to go about our everyday lives. We must encourage and incentivize new technical cyber security training for individuals and businesses to secure their computer systems. To keep technology progressing, the US government's research funding must be increased. The United States generates less scientists, engineers, physicians, and technicians than China and India, according to the World Future Society. That puts the United States at a disadvantage in the technical warfare (Citron, Davies, 2009). Being proactive, as well as continuing to improve AI and QC, will send a message to the rest of the world that the US will be a major participant until it reaches supremacy.

Evolution of quantum computing for cyber security

Roadmap to quantum computing for cyber security until today

Based on quantum mechanics principles, quantum computers employ fast evolving technology to handle complicated algorithms with ease. Because quantum computers can do certain sorts of computations faster than conventional computers, they may represent a substantial threat to current cryptographic cybersecurity solutions. This is why quantum-enabled cybersecurity is required.

Quantum computing holds the potential to unlock secrets ranging from one’s personal finances to a nation’s defiance strategy. Large-scale quantum computers, if realized, can enable hackers and nation states to break current cryptographic protocols.

In essence, they are capable of jeopardizing the security of widely used public key cryptosystems and revealing flaws in today's core digital systems, which enable a variety of internet services such as online financial transactions, e-commerce, and secure communications. **[20]**

https://www.openaccessgovernment.org/quantum-enabled-cybersecurity/141549/

Road Map: An Action Agenda to Advance Cybersecurity in the Quantum Era

Bring together experts from the security, quantum computing, government, and commercial sectors to determine how the impact of quantum computing on cybersecurity would influence the digital ecosystem.

Other recommendations emphasize the need of identifying individual risks and switching to quantum-resistant encryption for government organizations and businesses. These steps are required, yet they are insufficient. With the digital ecosystem's rising scope, complexity, and interdependence, the risks are systemic and must be addressed as such. Isolated mitigation creates holes and vulnerabilities in the system; the system must be fortified throughout all processes, supply chains, and common infrastructure. The government should bring together key experts in this field to investigate the dispersed and systemic threats of quantum computing.

Determine quantum vulnerabilities

Given how heavily society relies on current public-key cryptography systems for communications, data, and digital transactions, organizations must assess their existing procedures and infrastructure in order to prioritize risks and weaknesses. Businesses should engage time and money in a quantum risk assessment, similar to the government-level methodology mentioned above. Elements of this evaluation may overlap with what firms already do in terms of cyber security planning, such as recognizing the nature of their sensitive information, access control and data sharing agreements, backup and recovery methods, and end-of-life procedures. As part of their risk assessment, businesses should analyze their reliance on vendors' and suppliers' cybersecurity safeguards. **[21]**

https://www.belfercenter.org/publication/quantum-computing-and-cybersecurity

NIST Post-Quantum Cryptography standardization process

Concerned about the potential threat these machines pose to the security of data across government and private organizations, the United States National Institute of Standards and Technology (NIST) has been working with the cryptographic community since 2017 on the post-quantum cryptography standardization process to combat cyber threat actors, including those who are now operating under the concept of "harvest now, decrypt later." This means that encrypted material that is secure from existing cyber threats can be saved or captured today utilizing quantum susceptible methods and then decoded when large-scale practical quantum computers become available.

The NIST process has begun to analyze and define new public key cryptography standards, as well as specify at least one publicly published digital signature, public-key encryption, and key-establishment method. On July 5th, 2022, NIST concluded the third phase of the Post-Quantum Cryptography (PQC) standardization process, during which it selected four new algorithms to survive the threats posed by quantum computers.

Applications of Quantum Computing to Charged Particle Pattern Recognition

Before being used for physics analysis, raw data acquired by detectors is processed by reconstruction algorithms. Typically, the track reconstruction algorithms used to recover the paths of charged particles passing through tracking detectors are the most computationally intensive. The computational resources required for such methods grow roughly quadratically with the quantity of charged particles per event, i.e. the amount of pile up, and will therefore become even more difficult at future colliders. As a result, new concepts and methodologies for track reconstruction algorithms are now being developed in order to fully use the physics capabilities of the HL-LHC and beyond.

Global and local approaches to track rebuilding can be distinguished. Global algorithms process all of the data, or detector hits, from an event at the same time and provide a collection of tracks. Local algorithms are designed to identify the set of hits associated with a particular track and are repeated multiple times to identify the whole collection of songs. The Hough transform and neural networks are two examples of global techniques. The Kalman filter is the most extensively used local approach, and there has lately been substantial research into the usage of Graph Neural Networks (GNNs)

The method divides the detector hits into doublets and then triplets. A QUBO is made up of triplets, and the purpose is to figure out which pairs of triplets may be merged to produce quadruplets. Because triplets from the same track are anticipated to have identical properties, the weights in the QUBO are determined by the compatibility of the attributes of the triplets, particularly their curvature and the angles between them. On the quantum annealer, the QUBO is reduced by picking triplet combinations that are consistent with the paths of charged particles. However, due to the restricted amount of qubits accessible on today's quantum computers, the QUBO is broken into smaller sub-QUBOs that are solved separately using fewer qubits. qbsolve is a software application. This splitting is performed using D-Wave, and the solved sub-QUBOs are recombined to get the global minimum. Following minimization, a last post-processing step on a traditional computer is undertaken to transform the acceptable triplets back to doublets. Duplicates and doublets that have unresolved disputes with other doublets are eliminated. To limit the contribution from random combinations of hits, or fakes, the final track candidates must have at least five hits.

The algorithm was tested using the TrackML dataset, but just on the core portion of the detector, or barrel, which has a simpler shape and less material, making it an easier challenge for pattern recognition algorithms to solve. Furthermore, events were filtered to pick certain fractions of particles to simulate datasets with varying degrees of build up. This enables the performance to be analyzed in relation to the quantity of build up. The performance of quantum annealers was evaluated using simulations on Cori, a supercomputer at the National Energy Research Scientific Computing Center (NERSC), and quantum annealing hardware from D-Wave. The Ising D-Wave 2X at Los Alamos National Laboratory and the D-Wave LEAP cloud service, which is an interface given by D-Wave that allows users to operate on a variety of other quantum computers, were employed as quantum annealers. **[22]**

https://www.frontiersin.org/articles/10.3389/fphy.2022.864823/full

Successful implementation of complete quantum cryptography

Using the BB84 quantum cryptography protocol, the University of Cambridge and Toshiba Corp. developed a high-bit rate QKD system.

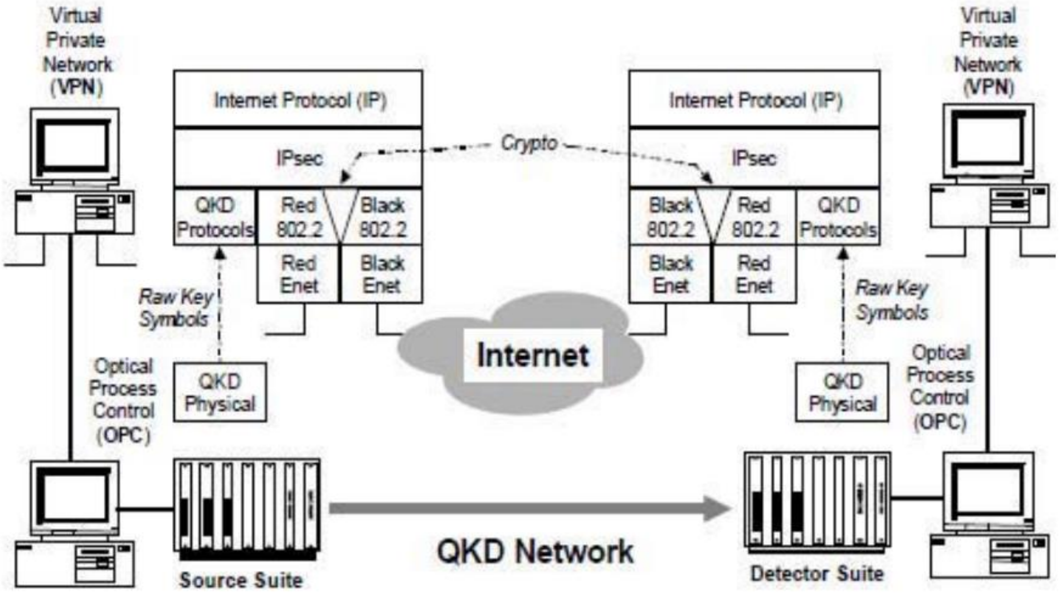
From 2002 until 2007, the Defense Advanced Research Projects Agency Quantum Network was a 10-node QKD network created by Boston University, Harvard University, and IBM Research.

Quantum Xchange established the first quantum network in the United States, consisting of 1,000 kilometers (km) of fiber optic cable.

Commercial QKD systems have also been developed by ID Quantique, Toshiba, Quintessence Labs, and MagiQ Technologies Inc.

In addition to QKD, the following protocols and quantum algorithms are commonly employed in quantum cryptography **[23]**

https://www.techtarget.com/searchsecurity/definition/quantum-cryptography



VPN Network Quantum Cryptography **[24]**

https://fardapaper.ir/mohavaha/uploads/2017/12/Fardapaper-Quantum-Cryptography-and-Quantum-Key-Distribution-Protocols-A-Survey.pdf

How to evaluating Artificial Intelligence Cybersecurity

This policy brief examines the fundamental concerns in seeking to enhance artificial intelligence cybersecurity and safety, as well as policymakers' involvement in addressing these challenges.

In January 2017, a group of artificial-intelligence experts assembled at the Asilomar Conference Grounds in California to produce the Asilomar AI Principles, a set of 23 principles for artificial intelligence (AI). "AI systems should be safe and secure throughout their operational lifetime, and verifiably so when appropriate and practicable," reads the sixth criterion. Thousands of professionals in academia and the corporate sector have now signed on to these principles, but many issues remain more than three years after the Asilomar meeting regarding what it means to make AI systems safe and secure. Verifying these properties in the context of a fast evolving sector and extremely complex deployments in areas like as health care, financial trading, transportation, and translation, among others, complicates the task.

Much of the debate so far has focused on how useful machine learning algorithms may be for discovering and fighting against computer-based vulnerabilities and threats by automating the detection and response to attempted assaults. Concerns have been expressed that employing AI for offensive goals may make cyberattacks more difficult to detect and defend against by allowing malware to adapt quickly to limits imposed by countermeasures and security controls. These are also the circumstances in which many policymakers consider the security implications of AI.

A similar but different set of questions is how AI systems can be protected in and of themselves, rather than merely how they may be utilized to increase the security of our data and computer networks. The urge to adopt AI security solutions in response to fast emerging threats heightens the need to safeguard AI itself; if we rely on machine-learning algorithms to identify and respond to cyberattacks, it is critical that such algorithms be secured against interference, compromise, or misuse. As we become increasingly reliant on AI for vital tasks and services, there will be more incentives for attackers to target those algorithms, as well as the possibility of each successful assault having more severe effects.

This policy brief examines the fundamental concerns in seeking to enhance artificial intelligence cybersecurity and safety, as well as policymakers' involvement in addressing these challenges. Congress has previously expressed interest in cybersecurity legislation aimed at certain types of technology, such as the Internet of Things and voting machines. As AI becomes a more essential and extensively utilized technology in a variety of industries, governments will be forced to confront the convergence of cybersecurity and AI. This article discusses some of the challenges that have arisen in this field, such as the hacking of AI decision-making systems for malevolent purposes, the possibility of adversaries gaining access to secret AI training data or models, and legislative solutions to address these concerns. **[25]**

https://jpt.spe.org/how-improve-cybersecurity-artificial-intelligence?gclid=Cj0KCQjw48OaBhDWARIsAMd966BjIJXSnBrGu1Gx6c-gweU8nsBtusxNsCML_OTB7YXMWLItyf0RbiIaAgiuEALw_wcB

Future for quantum computing and AI for cyber security

When Will Quantum Computing Come?

McKinsey & Company notes in their recent study "The Next Tech Revolution: Quantum Computing" that quantum computing is still in its infancy. However, it is projected that businesses such as banking will begin to benefit from quantum computing by 2025. Other industries are anticipated to follow suit as it becomes more accessible via the cloud or on its own.

According to McKinsey & Company's forecasts for the introduction of quantum computing, it is more feasible to assume a lengthier time period of at least 10 years until it reaches mainstream use. It is anticipated that the globe will have 2,000 to 5,000 quantum computers by 2030. However, due to the multiple pieces of technology and software necessary, it may be 2035 before these solutions are available to address commercial challenges. The banking industry is likely to profit the most from the arrival of quantum computing. **[26]**

https://www.cryptomathic.com/news-events/blog/when-will-quantum-computing-arrive-and-how-will-it-impact-cybersecurity

Quantum Computing Expected Impact for Cybersecurity

While quantum computing is predicted to alter businesses, particularly banking, it will also transform cybersecurity. Even though quantum computing is not projected to become ubiquitous until 2030 or later, organizations should start planning for its arrival today. Why? It is expected that quantum computers will someday be capable of factoring prime numbers used with asymmetric encryption methods, which form the foundation of existing data security systems, implying that it is time for enterprises to reevaluate their cryptography systems.

While quantum computing is expected to disrupt industries, notably banking, it is also expected to change cybersecurity. Even though quantum computing is not expected to become widely available until 2030 or later, businesses should begin planning for its arrival now. Why? It is believed that quantum computers will one day be capable of factoring prime numbers when employed with asymmetric encryption methods, which now form the backbone of present data security systems, meaning that it is time for businesses to review their cryptography systems. **[27]**

https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography

How could quantum computing affect cybersecurity?

Fortunately, many mathematicians in academia and government are working on a variety of prospective "quantum-resistant" algorithms that cannot be cracked by quantum computers.

New standards must be written and adopted, many of which are national or industry-specific; applications must be adapted to use the new algorithms, which can be difficult in some industries (such as banking) where there is a large amount of legacy infrastructure that cannot be easily upgraded, if at all.

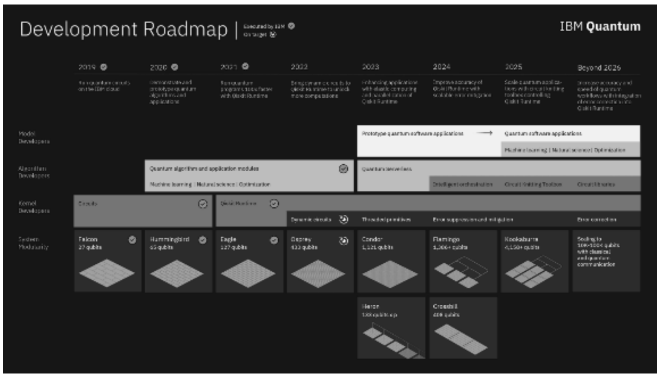
Algorithms like as DES, MD5, SHA-1, and RSA-512 are still used in certain places, but are thought to be breakable with classical computing now or in the near future due to the amount of inertia in big commercial systems where interoperability is critical.

So, given the foregoing and the most optimistic predictions of the availability of large quantum computers, there isn't much time to waste in starting to solve these problems!

The Post-Quantum Universe

Finally, the threat of quantum computing is reduced to an economic issue. Viable quantum computers will be incredibly expensive and have limited power at first, thus only governments will be able to purchase them and will only be able to attack the most important secrets of other nation states.

This power will gradually trickle down to organized criminals, but they will only be able to assault the most lucrative targets (e.g. falsifying financial transactions, blackmailing large companies or selling their sensitive data to the highest bidder). Hopefully, by the time quantum computing is widely available (if ever), the old, susceptible algorithms will have all but vanished.



Roadmap for development Quantum computing in IBM **[28]**

How are Quantum Computers Relevant to IT Security?

Probably not, because it is a worldwide issue with many individuals working on it. That doesn't mean you should disregard it. Keep a watch on the growth of quantum computing, the development of quantum-resistant algorithms, and the introduction of new standards; verify that your apps and infrastructure are upgradeable; prepare ahead of time and be ready to move.

(Note that the most recent Elliptic Curve technology gives no benefit - in fact, it's much less secure in the face of quantum computing - so there's no practical need to switch from RSA to ECDSA unless you require the performance benefits it provides.)

However, much encrypted information available today or in the coming years will almost certainly be susceptible to decryption one day in the future once quantum computers become widely available - all an attacker needs to do is capture the encrypted data today, including the initial key exchange handshake, and then wait until they have a quantum computer powerful enough to break it within a reasonable amount of computing time.

This is particularly a concern for governments, who have vast volumes of secret material with a lengthy "intelligence life," meaning it must be kept secret for at least 25 years for national security reasons. This is why governments are leading the research effort to create quantum computers for offensive cyber operations as well as quantum-resistant algorithms for defensive reasons. As there is a huge military advantage to be gained, they may even have clandestine research operations that are ahead of the academic community.

Commercial organizations with sensitive data that they want to protect in the long term and that are attractive targets for hackers should use symmetric algorithms with long key lengths (e.g., AES-256 rather than AES-128 or 3DES) as soon as possible, and use perfect forward secrecy techniques to minimize the amount of data protected under each key where Diffie-Hellman is used to negotiate symmetric keys.

They should also aim to transition to quantum-resistant algorithms as soon as possible. However, given the immaturity of such algorithms, it might be prudent to utilize hybrid methods at first (which combine proven, established algorithms with unproven, quantum-resistant algorithms, such that an attacker has to break both to be successful).

For the most paranoid, safety can be attained by completely avoiding public key encryption and relying solely on symmetric cryptography. However, this poses a new and perhaps more difficult security challenge: the secure exchange of secret key material. Maybe quantum key distribution will solve the problem. [29]

https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography

What Does the Future Hold for AI in Cybersecurity?

A solid defense against cyber-attacks requires a trained and experienced cybersecurity personnel, which is difficult to obtain given the high demand. The number of people interested in taking cybersecurity courses is growing. This tendency is projected to continue in the future, since demand much outnumbers supply.

If left unmanaged, cyber-attacks will grow in frequency and severity. This may be avoided by investing heavily in people on an ongoing basis. This may be accomplished by either recruiting cybersecurity professionals or teaching personnel on the use of AI in cybersecurity systems.

PECB provides ISO/IEC 27032 Cyber Security training courses to assist you in protecting and sustaining the long-term viability of business operations.

Certified personnel may create policy frameworks to identify procedures that are vulnerable to cyberattacks and guarantee that the organization is safe. [30]

https://pecb.com/article/artificial-intelligence-and-cybersecurity-what-the-future-holds

Conclusion

Computing requires the most rapid cyber security method to boost defense against attackers while also utilizing rapid processing mechanisms, in this scenario, quantum computing power may assist in making a rapid defense against attackers while also maximizing cyberspace safety. Artificial intelligence can be used to create an automatic defense system, and quantum cryptography mechanisms can be used to maximize data transform protection. However, because quantum computing and AI technology are still in their early stages, sum methods are not fully established in a theoretical and quantum, AI algorithmically stable in the near future find out the most frequently unhackable full security system.

Bibliography

[1] G. Wright, "echtarget," [Online]. Available: https://www.techtarget.com/whatis/definition/quantum. [Accessed 24 10 2022].

[2] G. Wright, "techtarget," [Online]. Available: https://www.techtarget.com/whatis/definition/quantum. [Accessed 20 10 2022].

[3] "azure.microsoft," microsoft, [Online]. Available: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-quantum-computing/#introduction. [Accessed 24 10 2022].

[4] "evolutionq," [Online]. Available: https://evolutionq.com/quantum-safe-cyber-security-faq.html. [Accessed 24 10 2022].

[5] W. H. Freeman, "ncbi.nlm," in *Quantum computers*, London, 1994.

[6] "SearchSecurity," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/quantum-cryptography. [Accessed 24 10 2022].

[7] "evolutionq," [Online]. Available: https://evolutionq.com/quantum-safe-cyber-security-faq.html. [Accessed 24 10 2022].

[8] "cloud.google," google, [Online]. Available: https://cloud.google.com/learn/what-is-artificial-intelligence.

[9] A. Tilbe, "towardsai," medium.com, [Online]. Available: https://pub.towardsai.net/the-future-of-ai-is-quantum-computing-10-of-the-most-important-use-cases-3a4b50c58f3e.

[10] "analyticsinsight," [Online]. Available: https://www.analyticsinsight.net/ai-and-quantum-computing-in-securing-the-cyberspace/.

[11] R. V. Loon, "simplilearn.com," [Online]. Available: https://www.simplilearn.com/quantum-computing-article.

[12] R. Morrison, "techmonitor.ai," [Online]. Available: https://techmonitor.ai/technology/emerging-technology/quantum-computing-regulation-ai.

[13] B. Marr, "forbes.com," [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/?sh=6b6a83c92404.

[14] R. Morrison, "techmonitor.ai," [Online]. Available: https://techmonitor.ai/technology/emerging-technology/quantum-computing-regulation-ai.

[15] C. REEDY, "Futurism," [Online]. Available: https://futurism.com/ai-and-quantum-computers-are-our-best-weapons-against-cyber-criminals.

[16] IBM, "ibm.com," [Online]. Available: https://www.ibm.com/watson/about.

[17] [Online]. Available: https://www.slideteam.net/quantum-computing-it-cybersecurity-and-cryptography-with-quantum-computing-ppt-skills.html.

[18] E. K. Petros Wallden, "cacm.acm.org," Communication of the ACM, [Online]. Available: https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext.

[19] M. S. D. J. Katie Kline, "iwp.edu," [Online]. Available: https://www.iwp.edu/cyber-intelligence-initiative/2019/03/27/how-artificial-intelligence-and-quantum-computing-are-evolving-cyber-warfare/.

[20] L. Barnes, "openaccessgovernment," [Online]. Available: https://www.openaccessgovernment.org/quantum-enabled-cybersecurity/141549/.

[21] M. Lee, "Road Map: An Action Agenda," in *Quantum computing and cybersecurity* , United States of America, 2021, p. 34.

[22] frontiersin, "frontiersin.org," [Online]. Available:

https://www.frontiersin.org/articles/10.3389/fphy.2022.864823/full.

[23] A. S. Gillis, "www.techtarget.com," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/quantum-cryptography.

[24] D. B. V. V. ,. D. A. V. N. K. Ms. V. Padmavathi, "VPN Network Quantum Cryptography," in *Quantum Cryptography and Quantum Key Distribution*, IEEE, 2016.

[25] The Brookings Institution Data Science and Digital Engineering, "jpt.spe.org," 09 06 2020. [Online]. Available: https://jpt.spe.org/how-improve-cybersecurity-artificial-intelligence?gclid=Cj0KCQjw48OaBhDWARIsAMd966BjIJXSnBrGu1Gx6c-gweU8nsBtusxNsCML_OTB7YXMWLItyf0RbiIaAgiuEALw_wcB.

[26] D. M. Turner, "cryptomathic.com," 21 06 2022. [Online]. Available: https://www.cryptomathic.com/news-events/blog/when-will-quantum-computing-arrive-and-how-will-it-impact-cybersecurity.

[27] R. Stubbs, "cryptomathic.com," 29 04 2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography.

[28] ibm.com, "ibm.com," ibm, [Online]. Available: https://www.ibm.com/quantum/roadmap.

[29] R. Stubbs, "cryptomathic.com," [Online]. Available: https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography.

[30] PECB, "pecb.com," 02 12 2021. [Online]. Available: https://pecb.com/article/artificial-intelligence-and-cybersecurity-what-the-future-holds.

[31] "The impact of online marketing in today’s world," [Online]. Available: https://www.researchgate.net/publication/358284346_DIGITAL_MARKEING_AND_ITS_IMPACT_IN_TODAYS_WORLD.

[32] "Components of a Successful Online Marketing Strategy," [Online]. Available: https://aspireinternetdesign.com/integrated-emarketing/6-components-of-a-successful-online-marketing-strategy/.

[33] "Online marketing," [Online]. Available: https://www.techopedia.com/definition/26363/online-marketing.

[34] "Cardinal Online marketing," [Online]. Available: https://www.cardinaldigitalmarketing.com/blog/top-9-benefits-of-digital-marketing/.

[35] "What is online marketing," [Online]. Available: https://www.tutorialspoint.com/online_marketing/online_marketing_introduction.htm#:~:text=Online%20marketing%20is%20advertising%20and,to%20facilitate%20the%20business%20transactions.

[36] "What does online marketing mean," [Online]. Available: https://www.techopedia.com/definition/26363/online-marketing.

[37] "Traditional marketing," [Online]. Available: https://intellipaat.com/blog/traditional-marketing-vs-digital-marketing/.

[38] "Comparision chart traditional and online marketing," [Online]. Available: https://keydifferences.com/difference-between-traditional-marketing-and-digital-marketing.html.

[39] "Defintion advantagfes and disadvantages," [Online]. Available: https://adilblogger.com/advantages-disadvantages-online-digital-marketing/.

[40] "Advantages and disadvantages for customers," [Online]. Available: https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-digital-marketing.

[41] "advantages for customers," [Online]. Available: https://www.webfx.com/digital-marketing/learn/how-does-digital-marketing-benefit-consumers/.

[42] "Online marketing Disadvantage for customers," [Online]. Available: https://digitalcatalyst.in/blog/what-are-the-main-advantages-and-disadvantages-of-digital-marketing/.

[43] "Online marketing advantages and disadvantages for business," [Online]. Available: https://adilblogger.com/advantages-disadvantages-online-digital-marketing/.

[44] "Most effective digital marketing techniques according to marketers worldwide in 2020," [Online]. Available: statista.com/statistics/190858/most-effective-online-marketing-channels-according-to-us-companies/.

[45] [Online]. Available: www.google.com.

[46] N. W. a. H. Klein. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/52464497/Artificial_Intelligence_in_Cybersecurity-with-cover-page-v2.pdf?Expires=1665317165&Signature=DVkBzIbmG3nit5jyCxDRsBzF6cWC4~5xQ~nGaS0xCazOCJCdfWQr2NntiwTXBEd~cvjt9Oi1PO2ndbwz2vQRu1khD~aej~zFucGMlHM1z1dW~akumtL.

[47] S. K. H. Jahankhani, Cyber defence in the age of AI.

[48] E. Segal, "The Impact of AI on Cybersecurity | IEEE Computer Society," [Online]. Available: https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity..

[49] K. Chadd, The history of cyber security, 2019.

[50] "10 Types of Cyber Attacks You Should Be Aware in 2022," [Online]. Available: https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks.

[51] "ARTIFICIAL INTELLIGENCE," [Online]. Available: https://onpassive.com/blog/artificial-intelligence-in-cybersecurity/.

[52] "Artificial Intelligence – Emerging Opportunities," [Online]. Available: https://scipol.duke.edu/printpdf/content/gao-report-artificial- intelligence-%E2%80%93-emerging-opportunities-challenges-and-implications .

[53] M. Rademaker, Assessing Cyber Security Information & Security, 2015.

[54] G. Press, "A Very Short History Of Artificial Intelligence (AI)," [Online]. Available: https://www.forbes.com/sites/gilpress/2016/12/30/a-very-short-history-of-artificial-intelligence-ai/?sh=626d017e6fba.

[55] "Number of internet and social media users worldwide as of July 2022," [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,the%20internet%20via%20mobile%20devices.

[56] K.Bhatele, The Role of Artificial Intelligence in Cyber Securit, 2021.

[57] R. Anyoha, "The History of Artificial Intelligence," [Online]. Available: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

[58] [. G. Bruneau, "The History and Evolution of Intrusion Detection," [Online]. Available: https://www.sans.org/white-papers/344/.

[59] T. F. Lunt, "A Real- Time Intrusion- Detection Expert System (IDES)," [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1666 .

[60] "evolutionq," [Online]. Available: https://evolutionq.com/quantum-safe-cyber-security-faq.html. [Accessed 24 10 2022].