ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 10, Issue 2, pp: (21-34), Month: April - June 2022, Available at: www.researchpublish.com

Post-Quantum Computing Technologies Intensifying Nation State Conflict: An Analysis of Quantum Based Cybersecurity Innovations and Adoptions

Andrew Vance[1]

[1]Senior Researcher, Cyber Institute, Center for Cyber Risk Research & Policy, New York, NY 10003

[1]Doctoral Candidate, Capitol Technology University, Quantum Computing Department, Washington D.C., 20708

Published Date: 08-April-2022

Abstract: **Emerging technologies are principal factors facilitating the predicted transformative changes that the Fourth Industrial Revolution is anticipated to generate during the 21st Century. Quantum computing is an emerging technology accelerating and necessitating innovations in cybersecurity. This quantitative and qualitive research analyzed current innovations involving quantum-computing-based cybersecurity and their implications for national security. We reviewed relevant post-quantum schemes against current technologies, emerging technologies, and standards; our evaluation derived the characteristics of those schemes towards their potential impact on the global community. The study further examined how quantum superiority has introduced a quantum arms race among nations seeking supremacy and how it intensifies the probability of nation-state conflict. Our findings and recommendations revealed an alarming research and adoption gap between quantum-computing-based cybersecurity and other quantum research. The research's resulting recommendations identify apposite approaches for addressing national and international conflict.**

Keywords: **Cybersecurity, Emerging Technologies, National Security, Post-Quantum, Quantum Computing.**

I. INTRODUCTION

Technology, whether analog or digital, has always been and will always be a critical factor in geopolitical change. In the 21st Century, emerging technology is a principal factor in the "fourth industrial revolution" [1],[2]. It will provoke a change in the global order by challenging the authority, sovereignty, and capacity of governments. This transformation of geopolitical influence influences a range of government responses, each embedded in a nation's specific political structure, relative economic strength, and broader global ambitions. The emerging technologies developed in the fourth industrial revolution will force dominant governments to acknowledge and adapt to the realization that they may no longer be able to exert their superpower status and influence on the global stage. A specific emerging technology is poised to intensify nation-state conflict, quantum computing. Nation states achieving quantum supremacy, are envisaged to be considered 'cyber superpowers' analogous to the nuclear superpowers of the cold war [3].

Contemporary computers are designed and built by means of classical Newtonian mechanics [4]; future computers will be designed and built using quantum mechanics [5]. A contemporary computer, known also as a classical computer, processes data using the limited binary states of either a one or zero. Classical computers store data in those binary states as a binary digit or bit for short. Quantum computers store data in a quantum bit, or qubit for short is equivalent to the classical computer's bit. Except quantum computers process data using limitless states by exploiting the superposition principle, a fundamental feature of quantum mechanics. The superposition principle permits the storage of information as continuous variables rather than discrete, binary variables. Classical computers can only store data in 0s and 1s, and all the calculations they perform are effectively combinations of 0s and 1s. Quantum computers can store data as a probabilistic distribution of an infinite number of values between 0 and 1. If the problem to be solved is formulated in such a way that the results of non-relevant calculations cancel each other out, the correct answers can be quickly found from simultaneous calculations. Quantum computers will correspondingly be able to perform calculations and factoring operations more effectively than classical computers, this demarcates the definition of quantum supremacy [6].

Endeavoring to achieve ‘competitive-market supremacy’ [7] technology companies are investing heavily in the development of their quantum computers [8]. Quantum computers are fundamentally different from contemporary computers and supercomputers being used by technology companies such as Google, IBM, and Facebook. Google announced at the end of 2019, that their Sycamore quantum computer had performed a calculation in just a few minutes that would be practically impossible for their most powerful supercomputer to solve. Google’s competitor, IBM criticized the experiment and denied the significance of the results. Sycamore’s achievement nonetheless represents a key milestone in the development of quantum computing. Nation-states are also investing heavily in quantum computers (Fig. 1), endeavoring to achieve ‘geopolitical-quantum supremacy’ [9]. To date, the preponderance of nation state quantum development has consistently focused on cryptography [10]. Current encryption created using classical computing is vulnerable to impending quantum computing capabilities. It is projected that a single quantum computer would break the strongest of encryption schemes in less time than classical computers [11]. Nation states are currently developing post-quantum cryptography [10]. Development of quantum-resistant algorithms and technologies could provide a means of defense for nations, such a solution is not viable for those states without the economic or technological ability to defend against attackers using quantum computers. Due to the potentially devastating security compromises that could result from such an occurrence, governments around the world in the USA, China, Russia, and India have each invested billions of dollars into quantum computing research. While their total quantum computing budget is not known, China has spent $10 billion on their National Laboratory for Quantum Information Sciences alone. The United States has accelerated their research and development of quantum computing science and its applications in technology through the National Quantum Initiative Act (NQIA). The NQIA provided $1.275 billion in funding. The European Union and India have committed over $1 billion into the field, putting them in the top tier of countries invested in quantum computing (Fig. 1). Attempts to achieve quantum supremacy by industries or governments, intensifies tensions of international implications necessitating analysis of related cybersecurity consequences.

II. SCOPE AND METHODOLOGY

This study conducted an extensive qualitatively examination of data sourced from a retrospective review of published research, policy, and standards from authoritative resources. The scope was limited to current research obtained from IOP Science, IEEE Xplore, Science Direct, Google Scholar, Scopus, Academia, ResearchGate, and resources.data.gov to provide a current landscape in quantum computing, with emphasis on research involving cybersecurity. This survey is not an exhaustive list of all quantum research nor an introduction to the field. This research does not review the conceptions or misconceptions of quantum computing’s computational power; particularly compared to classical computing. Adequately abridged studies already exist [12]. The “unidentified problems” that are implicated due to quantum computing is the focus of this study. We made a concerted effort to focus on clarifying misconceptions and to identify underrepresented research.

III. PROBLEM STATEMENT

Quantum computing cybersecurity represents only a fraction of overall quantum computing research [13]. Cybersecurity is a broad field of study, only a fraction of it is concentrating quantum computing opportunities and risks; the most prominent being cryptography [14]. Cryptography is the practice of encoding information to secure a line of communication between two or more parties through an untrusted medium to ensure security and confidentiality. How secure this method is when implemented is contingent on the capabilities of current classical computing. As more powerful computers become available, the efficacy of the existing methods is predicted to be ineffective. Fundamentally, cryptography bases its security on the inability to devise an efficient solution to complex problems and the inability of a person or machine to compute quickly enough to a brute-force attack. Classical computers are by current standards ‘speedy’, but even with their speed, cryptographic standards with large enough keys size will take decades if not centuries to break. As computing power advances, the keys historically have increased in size to add additional complexity to ensure next-generation computers cannot break them. It is a historical solution that has been used for decades. However, with the exponential increase in computing power that quantum computing is projected to bring, this strategy will fail as quantum computers will use more efficient schemes such as Grover's and Shor's algorithms. To corroborate this belief, the National Security Agency (NSA) funded a project to build a quantum computer capable of running Shor's Algorithm, allowing them to decrypt and record private Internet communications. The NSA's interest supposes that a quantum computer running Shor's algorithm would be capable of surveilling communications in other countries with ease if the other countries in question have not implemented quantum encryption algorithms. There is an arms race amongst nations and corporations attempting to develop quantum computers; primarily between the United States, China, and the European Union [15]. In 2017, the U.S. National Institute of Standards and Technology launched a post-quantum cryptography project designed to identify quantum-resistant public-key cryptographic algorithms [16]. In 2019, cyberespionage between the USA and China over quantum technology reached a significant milestone. The University of Science and Technology of China (USTC) achieved quantum supremacy with their own optical quantum computer. U.S. intelligence revealed that the Chinese government was making systematic efforts to steal and exploit the USA's federally funded research in quantum technology [17]. To develop their own quantum technology workforce, China sent scientists to conduct research in leading quantum technology labs across the USA for training on the condition that they would return to China on demand. Later, the Chinese government would recall the scientists to China to work on their local quantum technology projects, allowing them to capitalize on the knowledge and expertise the scientists gained from their research experience in the U.S. In January 2020, USTC announced that it had engineered an 80 kilogram 'ground station' capable of communicating with quantum satellites in orbit around the Earth. Implicated was the USTC, the same university that achieved quantum supremacy days after Google pioneered the achievement. China now leads the international community in "non-hackable quantum-enabled satellites" and possesses the world's fastest supercomputers. Efforts to institutionalize international cooperation on cyber governance lag. This is largely due to states' reluctance to restrict their sovereign control of cyberspace and uncertainty remains regarding the overall economic and national security impact of quantum research and development. The technologies that are anticipated from quantum computing will play a role in national security concerns. Quantum computers capable of undermining current cryptography are likely at least a decade off, but they are already introducing risks which nation states need to confront. The United States has publicly announced that more research is required to understand the national security implications of quantum [18] but there is alarming incongruity between quantum computing research and accompanying cybersecurity solutions.

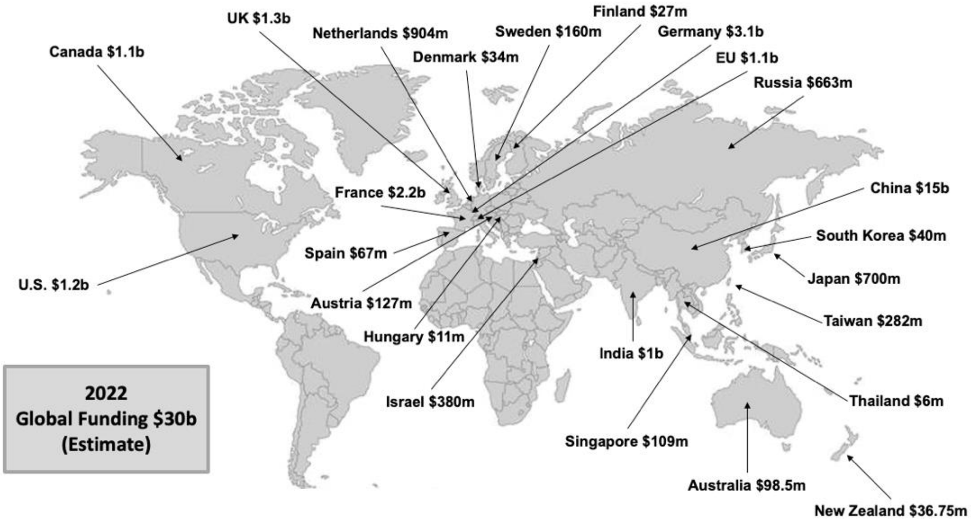

Figure 1: Estimated Quantum Funding Worldwide in 2022

IV. RESEARCH FINDINGS AND RECOMMENDATIONS

Our research revealed that quantum computing research and development is accelerating (Fig. 2). In 2022, IBM plans to release a 433-qubit processor called Osprey. By 2023, the company plans to release a 1,121-qubit processor called Condor. By the time Condor is released, IBM believes they will achieve quantum supremacy. In 2022, Microsoft plans to provide quantum access the cloud called Azure Quantum. This platform will provide companies access to quantum resources without the need for infrastructure and high expenses. The global quantum effort leading to research and innovation in quantum science and technology is continually rising with current worldwide investments reaching almost

$30 billion (Fig. 1). Overall, the global quantum technology market is projected to reach $42.4 billion by 2027 [19]. Quantum computing will lead the market at $16.1 billion by 2027 and 39.4% compound annual growth rate. North America will be the biggest regional market for quantum technologies overall. China will lead the Asian Pacific quantum technology market at $5.41 billion by 2027 with 38.5% compound annual growth rate. Germany will lead the European quantum technology market at $3.6 billion by 2027 with 33.1% compound annual growth rate [20]. In 2020, the White House stated that it intends to double non-defense quantum funding to $1.2 billion by 2022 [21].

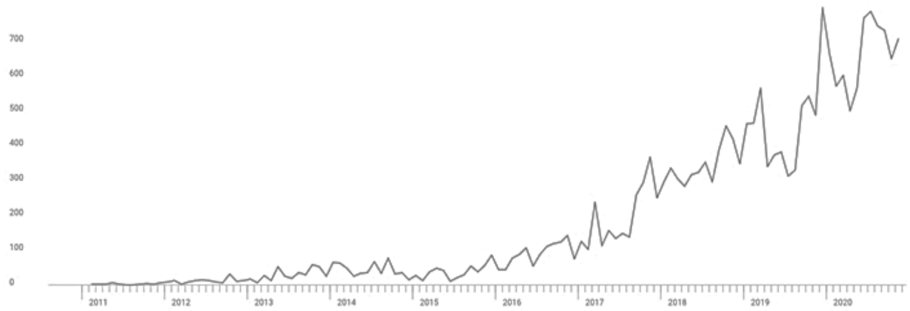

Figure 2: Quantum Computing Research Projects

The threat landscape is predicted to also accelerate. Researchers advise that the nation that first wins the quantum arms race will be able to protect their secrets with a higher level of security than other nation states and will have unconstrained access to those states that have lost it [22]. The scientific race is increasing towards quantum computing cybersecurity solutions with claims to solve high-margin problems previously intractable by conventional computational methods. Quantum computing innovations are predominately comprised of a synthesis of off-the shelf components with proprietary software and hardware [23]. The quantum race and capacity to mitigate against quantum threats, signifies a chronological extension of state power and advantage of global influence for first adopters [24]. The following research findings represents current innovations and implicit recommendations towards assuring nation state security.

Quantum Anti-Malware

Researchers have developed solutions using Qiskit framework as a basis for developing quantum computer programs that can be extended with the antivirus and pattern matching features [25] as well as implementing protocols approximating the "paranoid" classical protocols employed in military systems [26]. If quantum communication networks increase, they will likely be subject to a new type of attack by hackers, virus makers, and other malicious intruders. Research shows, it is possible to perform a fault injection attack using crosstalk on quantum computers when victim and attacker circuits are instantiated as co-tenants on the same quantum computer [25]. Attacks will target quantum logic gates, quantum states, and quantum algorithms. In comparison with classical information processing, there are more ways to attack quantum information processing, because due to superposition, quantum states contain more concurrent conditions than their classical counterparts. It is assumed quantum error correction will not be sufficient to detect quantum malware, as it is designed to deal with small errors. The same holds true for quantum dynamical decoupling [26] or other types of Zeno-effect like interventions [27]. Researchers introduce the concept of "quantum malware" [28]. Quantum malware may appear in the form of a quantum logic gate, or even as a whole quantum algorithm designed and controlled by the attackers. In comparison with classical information processing, there are more ways to attack in quantum information processing, because quantum states contain more degrees of freedom than their classical counterparts. The critical characteristic of quantum malware is that it would be comprised of quantum machine-language which encodes quantum logic gates and measurements. A prominent attack vector for quantum malware is to exploit the probabilistic protocol for quantum message authentication, secure quantum virtual private network, assumes that the sender and receiver are not subject to attacks by a third party at least while sending and measuring quantum states. The quantum aspect to this protocol preserves entanglement across the network. Defenders have access to three types of qubits; data qubits, which can be either online or offline; decoy qubits, which are online when the data qubits are offline; ancilla qubits, which are always offline. There six steps in the protocol, starting from the first network cycle (Fig. 3). The top row dots are data qubits, the middle row dots are ancillas, and the bottom row dots are decoy qubits. Initially (1), the system is offline. When data qubits are connected by straight lines (2), the system is online. The curly lines (2) represent entangled qubits. The time at which the network is turned on is random and unknown to the malware makers, and the duration too short for them to interfere. In the ultrashort step (3) the network is off and the state of data and ancilla qubits is swapped, as represented by the vertical straight lines. The decoy qubits may be under attack. (4) decoy qubits are subject to a malware attack. In all attacks, (5) the data and decoy qubits are reset, and the data qubits swapped with the ancilla qubits. Top row data qubits (6) indicate the end of a network cycle, and the start of a new cycle. Bottom part of the diagram illustrates the solution's timeline of the protocol. Improvement in the robustness of the stored quantum information is possible by replacing the SWAP operation with an encoding of each data qubit into a quantum error-detecting code. This enables the application for quantum fault tolerance and allows the defenders to check whether the data has been modified, via the use of quantum error detection.

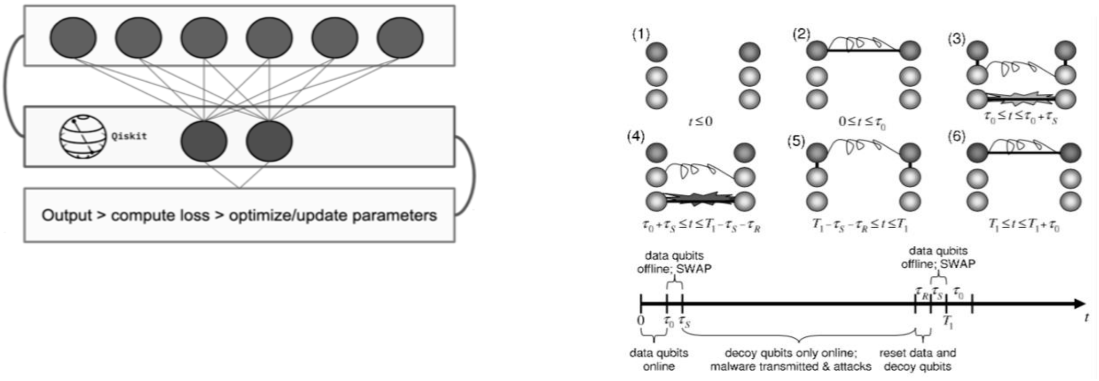
Qiskit
Output > compute loss > optimize/update parameters
(1)
$t \leq 0$
(2)
$0 \leq t \leq \tau_0$
(3)
$\tau_0 \leq t \leq \tau_0 + \tau_S$
(4)
$\tau_0 + \tau_S \leq t \leq T_1 - \tau_S - \tau_R$
(5)
$T_1 - \tau_S - \tau_R \leq t \leq T_1$
(6)
$T_1 \leq t \leq T_1 + \tau_0$
data qubits offline; SWAP
data qubits offline; SWAP
τ_R
τ_S
τ_0
0
τ_0
τ_S
T_1
t
data qubits online
decoy qubits only online; malware transmitted & attacks
reset data and decoy qubits

Figure 3: Qiskit Anti-Malware Extension and Qubit Based Anti-Malware Protocol

Quantum BotNet Detection

Scientists from the German Federal Ministry for Economic Affairs and Energy has funded work of hybrid quantum-classical deep learning model for cybersecurity applications such as botnet detection [29]. Quantum Artificial Intelligence (QAI) and Quantum Machine Learning (QML) are core components (Fig. 4) of the hybrid quantum deep learning to provide cybersecurity towards botnet detection [30]. Research results revealed that quantum deep learning model performed faster than the classical model: accuracy up to 94,7% (n=100) and 93,9% (n=1,000). While initial random seed values affected accuracy, the combination of Angle Embedding and Strongly Entangled ansatz delivered a high accuracy: maximum and average accuracy 94.7% and 91.4% respectively. The QML utilizes a parameterized quantum circuits (PQCs) approach with and added quantum layer between the Dropout and Dense layer. This hybrid quantum-classical generative model combines a parameterized quantum circuit with a classical neural net. The quantum Pennylane software framework provides an interface for quantum computers from providers such as IBM, Google, or Microsoft. The goal given for using a quantum computer in in the generator is that it is proposed that quantum computers can more efficiently sample from distributions classically loading and processing large amounts of high-dimensional data which is currently unsuitable for noisy intermediate-scale quantum (NISQ) devices. The overall quantum generator is given by Gq(z;θ,φ,ν) = W[gq(z;θ,ν);φ], z ∼ U(−π,π).

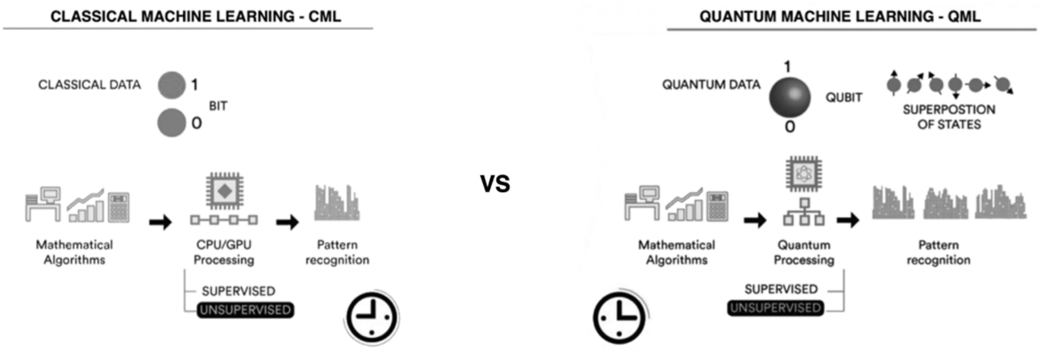

Figure 4: Quantum Based Botnet Comparative Efficiency

Quantum Key Exchanges

Currently, the most robust and prevalent quantum protocol is Quantum Key Distribution (QKD), which utilizes concepts from the Heisenberg's uncertainty principle and the no-cloning theorem to allow for two parties to communicate together securely over an unsecure channel. Quantum keys are then encoded bit-by-bit over single photons and transmitted as a stream of photons via a quantum channel, such as fiber-optic or free space optics. A hacker trying to intercept the photon stream in the quantum link will be unsuccessful. This is because any interruption or modification to the photons will alter the encoded state of the photon and therefore, causing detectable error. Using the quantum entanglement and superposition, the sender and receiver can set up a system to detect eavesdropping over the quantum channel. Based on the level of error that was caused by eavesdropping, the two parties can determine if the key has been compromised. If so, the sender and receiver can terminate their communication. The one major hurdle of QKD is that photon transmission is limited to approximately 60 miles, in which a network of trusted nodes needs to be created to allow keys to be shared over long distances and with multiple users. The two main protocols of utilizing QKD include BB84 and E91. Researchers have proposed that Supersingular Isogeny Diffie Hellman (SIDH) to overcome this limit. SIDH is a quantum robust key-exchange protocol that builds upon the concepts of elliptic curve Diffie Hellman (ECDH) [30]. The added complexity from ECDH is provided through isogeny, a morphism of algebraic groups. With classical computing elliptic curve cryptography (ECC), the security stemmed from the difficultly to determine the integer value, given two points on the same elliptic curve, A and C, such that C = nA. ECC isogeny conceptually is similar, with some added complexity. A function is created to map a point A in E1 to a point C in E2; this function is an isogeny (Fig. 5). For SIDH, the public key is the elliptic curve. The shared secret between the sender and receiver is the isogeny function. For key exchange, the sender and receiver mix their isogeny function with the public key to create a secret curve [31]. SIDH in the field of quantum-resilient cryptography is believed to have more robustness. The core idea in SIDH is to compose two random walks on an isogeny graph of elliptic curves in such a way that the end node of both ways of composing is the same. The black dots represent curves grouped in the same isomorphism classes represented by light circles (Fig. 6). Function 1 (e.g., Ea) takes the orange path ending up on a curve in a separate isomorphism class than Function 2 (e.g., Eb) after taking the dark blue path ending on Eb. SIDH is secure as it is parametrized in a way that Ea and Eb will always end up in different isomorphism classes.

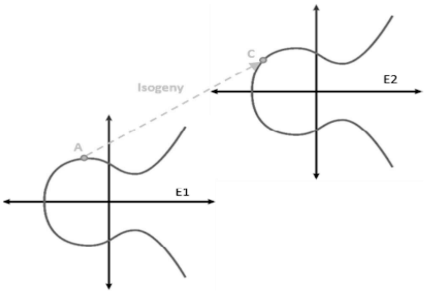

Figure 5: ECC Isogeny

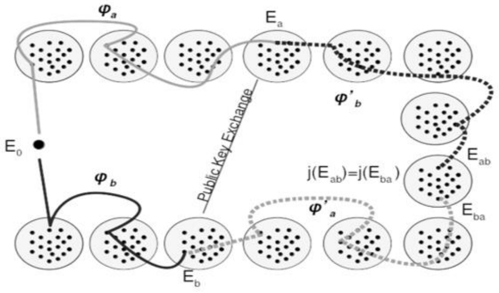

Figure 6: Supersingular Isogeny Diffie-Hellman

With quantum supremacy, comes the compromise the security of many commonly used cryptographic algorithms. Quantum computers are predicted to break many public-key cryptosystems, including RSA, DSA, and elliptic curve cryptosystems. These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks. Due to this concern, most of the quantum cybersecurity-based research involves post-quantum cryptography (PQC). To implement PQC, public-key cryptography is replaced with quantum key distribution (QKD). The main advantage of this approach is that the security relies not on any computational assumptions but the laws of quantum physics. In QKD, legitimate users have pre-shared authentication keys and control the communication channel. They establish a QKD protocol that allows them to obtain a raw quantum key, which contains some errors and some information about the key that is potentially known to the adversary. In the QKD security proofs, it is assumed that all errors in raw quantum keys are due to eavesdropping, users initiate the post-processing procedure using the authenticated public channel. As a result, users have a key for applications, which is proven to be theoretically secure against arbitrary attacks, including the quantum ones

[32]. QKD-generated keys can be used for conventional symmetric encryption, such as AES, and used to frequently refresh keys. The largest QKD network is by now deployed in China, which spans 4600 km and includes the link between the cities of Shanghai, Hefei, Jinan, and Beijing and a satellite link spanning 2600 km between two space observatories [33].

Quantum Firewalls

A quantum based virtual firewall was developed using quViCE (Quantum Virtual Computing Environment) and quC (Quantum Converter) components to provision quantum resources to architect a software firewall and to convert bits into quBits and quBits into bits (Fig. 7). The main problem quViCE attempts to address is virtual network traffic [34]. In many virtual networks when many virtual machines are connected the network traffic is going to a very high and sometimes because of that network traffic very important operations are delayed. The quantum virtual firewall allows managing the network security of the virtual infrastructure per-virtual machine basis, defining network traffic rules, and hardening the security of the quantum virtual computing environment. The firewall utilizes a Tree- Rule firewall technique, which filters packets in a tree-like way based on their attributes such as IP address and protocols. The proposed advantage of the quantum virtual firewall is that will provide power to control the bandwidth utilization of each virtual machine in the infrastructure, preventing overutilization and denial of service to critical applications due quantum incoherence, or the quantum noise problem [35]. The solution introduces Quantum Pseudo-Telepathy as a property of certain games which allows winning strategies only for players capable of using quantum information [36]. Topical studies tackle the question of the robustness of the effect against noise due to imperfect measurements on the coherent quantum state. Recent work has shown an exponential enhancement in the communication cost of nonlinear distributed computation, due to entanglement, when the communication channel itself is restricted to be linear.

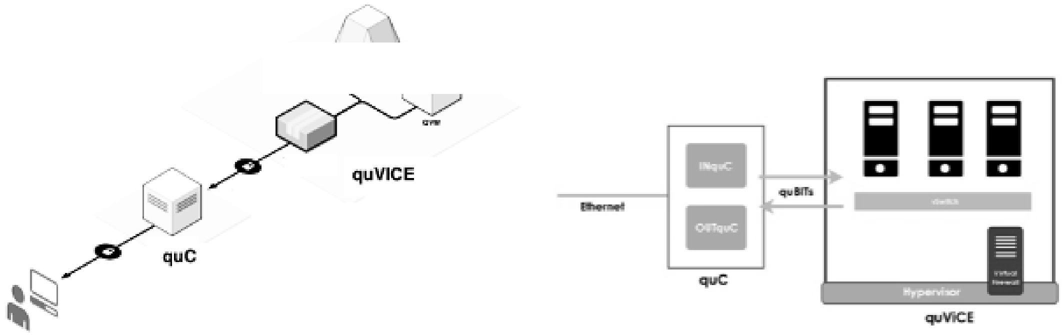

Figure 7: Quantum Based Firewall Components

Quantum Intrusion Detection Systems

Research on quantum beetle swarm algorithm optimized (QBSO) artificial intelligence and machine learning for intrusion detection leverages heuristic anomaly approach to improve detection accuracy (Fig. 8) [37]. Researchers explored Quantum Algorithms applied to Intrusion Detection Systems to propose Quantum Intrusion Detection System which is a fusion of classical and quantum techniques. Previous research proposed quantum vaccine immune clonal algorithm with the estimation of distribution algorithm (QVICA) as a replacement classification algorithm for the intrusion detection systems. It compared classification algorithm based on particle swarm optimization (PSO) on data sets to propose performance-based improvements higher classification accuracy than the best value of the PSO based algorithm using the same parameters [38]. Classification accuracy values obtained at the different experiments showed the ability of the algorithm of achieving high classification accuracy. Quantum Support Vector Machines, hybrid Quantum Classical Neural Networks, and a two-circuit ensemble model running parallel on two quantum processing units. Their work demonstrates quantum models' effectiveness in supporting current and future cybersecurity systems by obtaining performances close to 100%, being 96% the worst-case scenario [39]. QBSO combines the advantages of quantum computing and swarm intelligence algorithms to improve the k-means algorithm and make the k-means algorithm converge towards the global optimal direction. The proposed algorithm was tested on several standard datasets from University of California Irvine Machine Learning Repository for cluster analysis and its performance is compared with other well-known algorithms [40]. QVICA with the Estimation of Distribution Algorithm (EDA) was proposed to build a new Network Intrusion Detection System (NIDS). The proposed algorithm is used as classification algorithm of the new NIDS where it is trained and tested using the QVICA with EDA data set. The new NIDS was compared with a detection system based on particle swarm optimization (PSO) and results showed the ability of the proposed algorithm of achieving high intrusions classification accuracy where the highest obtained accuracy is 94.8 % [38]. The growth and development of solutions for the Internet of Things (IoT) has created issues that Quantum IDS is ideally suited [41].

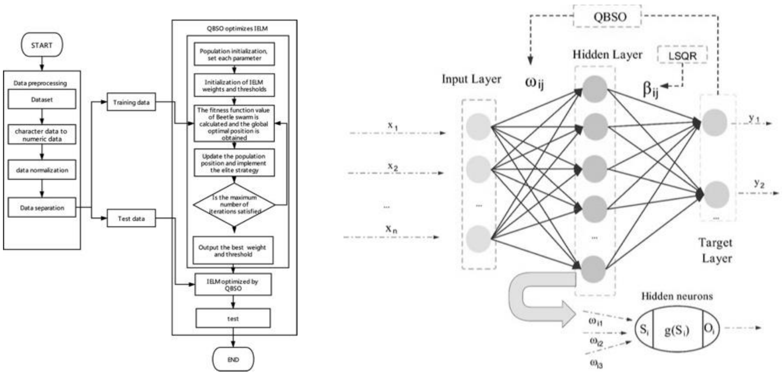
START
Data preprocessing
Dataset
character data to numeric data
data normalization
Data separation
Training data
Test data
QBSO optimizes IELM
Population initialization, set each parameter
Initialization of IELM weights and thresholds
The fitness function value of Beetle swarm is calculated and the global optimal position is obtained
Update the population position and implement the elite strategy
Is the maximum number of iterations satisfied
Output the best weight and threshold
IELM optimized by QBSO
test
END
QBSO
Input Layer
ω_ij
Hidden Layer
LSQR
β_ij
x_1
x_2
...
x_n
y_1
y_2
Target Layer
Hidden neurons
ω_i1
ω_i2
ω_i3
S_i
g(S_i)
O_i

Figure 8: Quantum Beetle Swarm Algorithm Optimized (QBSO)

Quantum Risk Analysis

The current method of choice for performing risk analysis is variance of the Monte Carlo simulation [42]. This classical method is useful when computing expectation values or risk measures of functions depending on random parameters. However, value at risk (VaR) calculations are computationally intensive due the width of the confidence interval scales. Many different runs are needed to achieve a representative distribution of the portfolio value. Amplitude estimation is a quantum algorithm used to estimate an unknown parameter and converges that are achieved more easily with quantum processing. The Monte Carlo method's convergence rate (i.e.: the rate at which the desired accuracy is approached) scales as the inverse of the square root of the number of samples (one sample corresponds to one set of parameter values). Researchers at IBM Quantum developed a quantum algorithm that converges at a rate proportional to the inverse of the number of samples. The innovation employed a quantum amplitude estimation to evaluate risk measures such as VaR and Conditional Value at Risk on a gate-based quantum computer. A Canadian company adopted the innovation to provide quantum risk assessments to prevent quantum security threats to their IT infrastructure. They propose a model for evaluating quantum risk using a six-phase process consistent with risk assessment models from NIST, and incorporates Mosca's "x, y, z" quantum risk model [43]. It provides a basis for an organization to address quantum risk proactively, to build a roadmap to a quantum safe state, and to implement and validate quantum safe solutions as part of normal life cycle management rather than as a response to a crisis. Quantum Fourier Transform is applied to measure state (Fig. 5) where the Hadamard gate denotes the inverse Quantum Fourier Transform on m qubits. This approach provided a significant increase in speed over established classical algorithms by speeding up risk assessment through quantum algorithms; a quadratic speedup compared with current method Monte Carlo simulations.

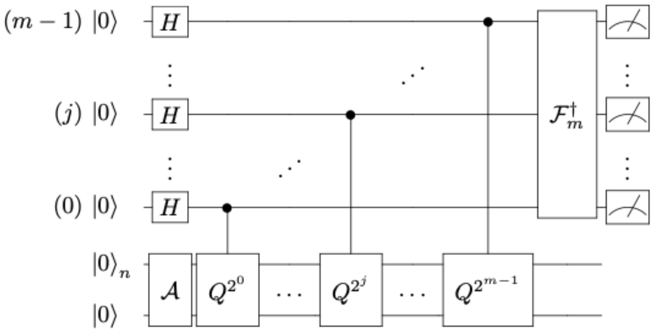

Figure 9: Quantum Circuit for Amplitude Estimation for Risk Analysis

V. DISCUSSION

Ten thousand eight hundred results were returned in Google Scholar for "post quantum cybersecurity solutions" search. Of those results, five hundred ninety-four (99.94%) were focused on some aspect of cryptography (to include blockchain). Globally there are 245 Quantum Computing startups and globally there are 66 quantum computing in cybersecurity companies of the top 10. However, all top 10 are quantum encryption [14]. Despite the promising developments in advances in quantum-proof encryption technology and innovations addressing theorized threats, quantum computing cybersecurity is still an emerging field with alarming gaps in research. While both quantum and post-quantum cryptography undergo active standardization processes [44], the standardization of the post-quantum cryptography currently is centered around the NIST initiative. NIST recognizes that some users may wish to deploy systems that use "hybrid modes," which combine post-quantum cryptographic algorithms with existing cryptographic algorithms, which may not be post-quantum and issued a call for proposals for standardization [45]. NSA Cybersecurity reviewed the security analysis and performance characteristics of the proposals. They advise that lattice-based schemes with strong dependence on well-studied mathematical problems and hash-based signatures are suitable for only certain niche solutions [46]. NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of Quantum Key Distribution (QKD) and PQC for securing the transmission of data in National Security Systems (NSS) unless limitations are overcome as they state systems capable of Quantum Key Distribution cannot be scaled efficiently and might not ever become widely available to consumers [46].

Even though research has made significant progress in cryptography, it has not addressed the security of data at rest [47]. While there has been innovations quantum computing cybersecurity, there is growing need for global cooperation regarding cyberattacks and cyberwarfare [48], [49]. Cyberwar is a reality. In 2007, Estonia suffered what was at the time the most comprehensive cyberattack in history. Using the method of "distributed denial-of-service" (DDoS), Russian-backed operatives maintained the assault for approximately twenty-two days, causing blackouts in Estonia's major commercial banks, telecoms, media outlets, and other essential government servers. An attack from a quantum computer could be fundamentally different [50]. The DDoS attack against Estonia was a form of technological carpet-bombing, a quantum computer attack can be far more precise, a clinically efficient sniper. In the future, quantum computers could not only be focused on denying access, infiltrating, and gaining access to steal, alter or destroy information, it could be used to exponentially effect destruction through quantum enhanced DDoS. Had a quantum computing attack been employed in Estonia in 2007, the citizens could have faced far greater consequences, potentially including the absolute loss of confidential information necessary for functioning in a national economy. Despite discourse on cyberwarfare and the law of international armed conflict since 2001 [51], it was not until the 2007 cyberattacks on Estonia that the international community moved to discuss cyberspace as a domain of war [52], [53]. Action was also a result, in response to those attacks, the North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallin, Estonia [54].

Congress should establish a national quantum research task force, analogous to the AI research task force that was established as part of the National AI Research Resource Task Force Act of 2020 [55]. This task force should be from academia, government, and industry and create a roadmap to establish a national quantum computing cloud that provides researchers with affordable access to high-end quantum computing resources in a secure cloud environment, as well as the necessary expertise they need to exploit this resource. The roadmap would be a first step in developing this resource by detailing how to build, deploy, fund, and govern a national quantum computing cloud. Congress should establish a National Quantum Research Cloud. Few researchers outside of government and large research corporations and organizations have access to quantum computers. Access to these systems through quantum clouds will increase research while also allowing policy pundits to observe trends in innovations to propose national security policies with greater emphasis on quantum computing cybersecurity.

VI. CONCLUSION

Quantum cyberwarfare has become a reality among nation states [56]. Quantum supremacy will be achieved [57]. There is a now greater need to address the impact of quantum computing on cybersecurity as the technology evolves. More focus needs to address cybersecurity and related policy. The apposite approach for the United States is the NSTC's Subcommittee on Quantum Information Science (SCQIS) which currently coordinates Federal research and development in quantum information science and related technologies. SCQIS should develop agency-level plans and policies to address gaps in quantum cybersecurity. This would foster new innovations and adoptions, such as those identified in this study, to better align transformative cybersecurity systems, including quantum-resistant cryptography, with wider developments in quantum computing. Quantum enabled security needs to assure nation states that this new, unprecedented computational power, is developed with the appropriate standards of accuracy, reliability, and privacy. While major efforts have been directed towards defining cyber operations within the scope of armed conflict, developed nations continue to experience substantial economic losses because of international cybercrime and cyberespionage. A report by the Center for Strategic and International Studies reports the economic costs of malicious cyber activity as averaging 0.8% of global gross domestic product. The use of cyber operations to economically cripple a nation appears to be a viable means of conducting cyberwarfare. The apposite international approach to preclude cyberwarfare is through updating an existing Treaty certified during the Budapest Convention [51]. The Budapest Convention was the Council of Europe's first regulatory instrument to address crimes committed via the internet and other computer networks. Also known as the Treaty 185: Convention on Cybercrime, it is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. Ratified in 2001, the treaty's main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime (CoE 2001). Due to the treaty's twenty-year legacy and eighty-plus signatories, it is the most effective instrument to advance international consensus and cooperation on quantum computing related cybersecurity. Nation states endeavoring to achieve 'geopolitical-quantum supremacy' will need to collectively identify strengths and focus areas, as well as gaps and opportunities, of international actors to better understand the evolving international quantum landscape from both technical and policy perspectives.

VII. FUTURE RESEARCH

Emerging technologies developed for commercial use are increasingly being proposed for defense, creating regulatory challenges. Protecting nation-state interests reply upon proper governance in development to prevent unintentional vulnerabilities from being exploited.

Although there have been large cryptographic research projects involving post-quantum security, our research found there is lacking projects focusing on blockchain. There are no post-quantum blockchain algorithms that provide, at the same time, small key size, short signature/hash sizes, fast execution, low computational complexity, and low energy consumption. Such factors are especially critical for resource-constrained embedded devices like the ones used with the IoT. Future research should focus on policies ensure compliance with laws and regulations, give guidance for decision-making, and streamline internal processes.

Since the 1950s, the United States has depended on its technological advantage as a key component of national security [58]. Careful consideration needs to be applied to ensure consistent application of existing classification and export control mechanisms will still provide the largest amount of information possible to American universities and industry about actions related to quantum research to encourage economic opportunities, protect intellectual property while still defending national-security-relevant interests. The growth in purely commercial technology can make it difficult to even identify which technology could have national security implications. Despite recent recommendations by defense experts and researchers, nation states need to address the prospect of weaponizing quantum computing and restrict export of key aspects of the technology. Exports of certain technologies are already limited under the International Traffic in Arms Regulations (ITAR) or Export but quantum computing currently is not. Under ITAR, the Department of State manages the export of dedicated military technologies with the United States Munitions List (USML), while its' schemes address international law frameworks that support nonproliferation of nuclear, chemical, biological, and missile technologies [59], there are currently no schemes adequately address quantum computing. Several bills have been introduced, but none passed, that would impose limits on the export of quantum technologies to China, including those related to quantum computing and simulation: China Technology Transfer Control Act of 2019, S. 1459, H.R. 3532; Fair Trade with China Enforcement Act, S. 2, H.R. 704; Uighur Intervention and Global Humanitarian Unified Response (UIGHUR) Act of 2019, H.R. 1025; and United States Export Finance Agency Act of 2019, H.R. 3407 (CRS, 2020). Research to propose new regulatory rules could help to overcome these challenges and effectively control potential threats from new technologies without stifling innovation.

REFERENCES

[1] K. Kitchen. "The New Superpowers: How and Why the Tech Industry is Shaping the International System". Insight from the Archives, A Project of National Affairs. No. 51, Spring 2022. Available online: https://nationalaffairs. com/the-new-superpowers-how-and-why-the-tech-industry-is-shaping-the-international-system

[2] World Economic Forum. "The Fourth Industrial Revolution: What it Means, how to Respond". Global Agenda Report. Jan. 14, 2016. Available online: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[3] S. Miller, R. Legvold, L. Freedman. "The Interplay Between the International System and the Global Nuclear Order: Nuclear Weapons in a Changing Global Order". Research Paper, American Academy of Arts & Sciences. Jan. 2019. Available online: https://www.amacad.org/publication/nuclear-weapons-changing-global-order/section/4

[4] G. Stibitz. "Early Computers: A History of Computing in the Twentieth Century". Academic Press, Bell Laboratories, New York. https://doi.org/10.1016/B978-0-12-491650-0.50034-4

[5] University of Waterloo. "Quantum Computing 101". Institute for Quantum Computing, May 17, 2013, Available online: https://uwaterloo.ca/institute-for-quantum-computing/quantum- computing-101

[6] Harvard Science Review. "The Race to Quantum Supremacy". Science in Society Review. Spring 2020. Available online: https://issuu.com/uchicagotth/docs/sisr_spring_2020/s/10648012

[7] R. D'Aveni. "Strategic Supremacy through Disruption and Dominance". Sloan Management Review Research, Massachusetts Institute of Technology. Apr. 15, 1999. Available online: https://sloanreview.mit.edu/article/strategic-supremacy-through-disruption-and-dominance/

[8] Quantum Computing Report. "Private Startup Companies; Quantum Computing and Quantum Communications". Where Qubits Entangle with Commerce, Quantum Computing Report. Feb. 2022. Available online: https://quantum computing report.com/privatestartup/

[9] D. Guy (2018). "The Weaponization of Quantum Physics: How Technology is Transforming Warfare". Technical Research Report, Defense Technical Information Center. Feb. 15, 2018.

[10] National Security Agency. "Post-Quantum Cybersecurity Resources". NSA Central Security Service. Available online: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

[11] Harvard Law School. (2018). A Quantum Leap in International Law on Cyberwarefare: An Analysis of International Cooperation with Quantum Computing on the Horizon. National Security Journal, Nov. 8, 2018

[12] P. Walden, E. Kashefi. "Cyber Security in the Quantum Era." Communications of the ACM, Apr. 2019, Vol. 62 No. 4, Page 12010.1145/3241037. Available online: https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext

[13] A. Vance, R. Campbell, T. Vance. "A Qualitative Meta-Analysis of Contemporary Research Correlating Post-Quantum Vulnerabilities and Opportunities to Cybersecurity". Journal of European Academic Science and Research, Vol. 1 No. 25, Feb. 28, 2022. ISSN 2789-1968

[14] Tracxn Technologies (2022). "Top Quantum Computing in Cybersecurity Startups". Trending Themes, Traxn. January 15, 2022. Available online: Tracxn Technologies

[15] M. Vermeer, E. Peet. "Securing Communications in the Quantum Computing Age". Rand Corporation. ISBN: 9781977404619. DOI: https://doi.org/10.7249/RR3102

[16] Harvard Law School. "A Quantum Leap in International Law on Cyberwarfare: An Analysis of International Cooperation with Quantum". National Security Journal, Harvard Law School. Nov. 2018. Available online: https://harvardnsj.org/2018/11/a-quantum-leap-in-international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/#_ftn40

[17] G. Mone. "The Quantum Threat". Communications of the ACM, Vol. 63 No. 7, Pages 12- 14 10. 2002. 1145/3398388

[18] Quoting Office of the President. “The White House predicts that a shared understanding about norms of acceptable cyber-behavior will bring predictability to state conduct, helping prevent misunderstandings that could lead to conflict”. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Nov. 8, 2012

[19] BCC Research. “Quantum Computing: Technologies and Global Markets to 2026”. Cloud Computing Market Research, BCC Research Publishing. Jan. 2022. ASDR-595893.

[20] Research and Markets. “Quantum Technology Market by Computing, Communications, Imaging, Security, Sensing, Modeling and Simulation 2022 – 2027”. Technology Market Research Report, Mind Commerce Publishing. Feb. 2022. MCMS-ID 5317365

[21] Congressional Research Service. “Quantum Information Science: Congressional Activity and Federal Policy Recommendations”. Apr. 28, 2020. Available online: https://www.everycrsreport.com/files/2020-04-28_IF11524_ 5006928af7f0284ebbb8ffc9 bd2a342e30a3fb44.pdf

[22] A. Majot, R. Yampolskiy. “Global Catastrophic Risk and Security Implications of Quantum Computers”. Futures No. 72, pages 17–26. Feb. 6, 2015. doi:10.1016/J.FUTURES.

[23] N. Kilber, D. Kasestle, S. Wagner. “Cybersecurity for Quantum Computing”. Quantum Physics, Cornell University. Oct. 27, 2021. doi: https://doi.org/10.48550/arXiv.2110.14701. Available online: https://arxiv.org/abs/2110.14701

[24] J. Tibbetts. “Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers”. Lawrence Livermore National Laboratory. LLNL-TR-790870. Sep. 20, 2019. Available online: https://cgsr.llnl.gov/ content/assets/docs/ QuantumComputingandCryptography-20190920.pdf

[25] S. Deshpande, C. Xu, et al. “Towards an Antivirus for Quantum Computers”, Cryptography and Security, Cornell University. 2022.doi: 10.48550/arXiv.2203.02649

[26] L. Wu, D. Lidar. “Quantum Malware”, Quantum Information Processing, Vol. 5, No. 2, Apr. 2006. doi: 10.1007/s11128-006-0014-5. Available online: https://www.researchgate.net/publication/2195486_Quantum_ Malware

[27] L. Viola, J. Mod. “Advances in Decoherence Control”. Journal of Modern Optics, Vol. 51, Issue 16-18, Pages 2357-2367. Feb. 15, 2004. https://doi.org/10.1080/09500340408231795

[28] P. Facchi, S. Tasaki, S. Pascazio, et al. “Control of Decoherence: Analysis and Comparison of Three Different Strategies”. Physical Review. Rev. A 71, doi: 10.1103/PhysRevA.71.022302

[29] D. Herr, B. Obert, M. Rosenkranz. "Anomaly detection with variational quantum generative adversarial networks". Quantum Science and Technology. Jul. 22, 2021. Available online: https://arxiv.org/pdf/2010.10492.pdf

[30] H. Suryotrisongko, Y. Mushasi. “Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection”. Science Direct, Procedia Computer Science, Vol. 197, Pages 223-229. 2022. https://doi.org/10.1016/ j.procs.2021.12.135. Available online: https://www.sciencedirect.com/science/article/pii/S1877050921023590

[31] B. Buchanan, “Supersingular Isogeny Diffie-Hellman (SIDH) for Post Quantum Computer Key Generation,” Medium, Mar. 22,2020. Available: https://medium.com/coinmonks/supersingular-isogeny-diffie-h ellman-sidh-for-post-quantum-computer-key-generation-6742 d2ea78dc.

[32] S. Yunakovsky, M. Kot, et al. “Towards Security Recommendations for Public-Key Infrastructures for Production Environments in the Post-Quantum Era”. EPJ Quantum Technology, 2021. https://doi.org/10.1140/epjqt/s40507-021-00104-z

[33] A. Chen, Q. Zhang, W. Cai, et al. “An Integrated Space-to-Ground Quantum Communication Network Over 4600 Kilometers”. Nature (London). 2021; 589:214.

[34] H. Amellal, A. Meslouhi, Y. Hassouni. et al. “A Quantum Optical Firewall Based on Simple Quantum Devices”. Quantum Information Processing Vol. 14, pages 2617–2633. May 5, 2015. https://doi.org/10.1007/s11128-015-1002-4

[35] D. Sooriyapala, G. Lakmal, et al. “QuViCE to Improve Virtual Firewall Performance”. International Journal of Scientific and Research Publications, Vol. 6, Issue 4, Apr. 2019. ISSN 2250-3153.

[36] G. Brassard, A. Broadbent, A. Tapp. “Quantum Pseudo-Telepathy”. Foundations of Quantum Physics, Cornell University. Vol. 35, Issue 11, Nov. 2005, Pages 1877 - 1907. Available online: https://arxiv.org/pdf/quant-ph/0407221.pdf

[37] Dong, Y., Hu, W., Zhang, J. et al. “Quantum Beetle Swarm Algorithm Optimized Extreme Learning Machine for Intrusion Detection”. Quantum Information Processing Vol. 21, Issue 9. 2022. doi:10.1007/s11128-021-03311-w

[38] O. Soliman, A. Rassem. “A Network Intrusion Detection System based on a Quantum Bio Inspired Algorithm”. International Journal of Engineering Trends and Technology, Vol. 10, No. 8, Apr. 2014. Available online: https:// arxiv.org/pdf/1405.1404.pdf

[39] E Payares, J. Martinez. “Quantum Machine Learning for Intrusion Detection of Distributed Denial of Service Attacks: A Comparative Overview”. Proceedings SPIE Vol. 11699, Quantum Computing, Communication, and Simulation. Mar. 5, 2021. https://doi.org/10.1117/12.2593297

[40] J. Chen, X. Qi, L. Chen, et al. “Quantum-Inspired Ant Lion Optimized Hybrid K-Means for Cluster Analysis and Intrusion Detection”. Knowledge-Based Systems, Science Direct, Vol. 203, Sep. 5, 2020. https://doi.org/10.1016/ j.knosys.2020.106167

[41] Y. Balasubramanian, D. Baggam, S. Venkatraman, et al. “Quantum IDS for Mitigation of DDoS Attacks by Mirai Botnets”. Smart and Innovative Trends in Next Generation Computing Technologies, Communications in Computer and Information Science, Vol 828. Springer, Singapore. Jun. 9, 2018. https://doi.org/10.1007/978-981-10-8660-1_37

[42] S. Woerner, D. Egger. “Quantum Risk Analysis”. Journal of Quantum Physics. Jun. 18, 2018. https://doi.org/ 10.1038/s41534-019-0130-6Available online arXiv:1806.06893.

[43] M. Mosca, J. Mulholland. “A Methodology for Quantum Risk Assessment”. Cybersecurity and Fraud Technology Innovations, Global Risk Institute. 2021. Available online: https://globalriskinstitute.org/download/a-methodology-for-quantum-risk-assessment-pdf/

[44] R. Campbell. “Evaluation of Post-Quantum Distributed Ledger Cryptography”. The JBBA, Vol. 2, Issue 1. 2019 ISSN: 2516-3949 https://doi.org/10.31585/jbba-2-1-(4)2019

[45] National Institute of Standards and Technology. “Post-Quantum Cryptography Standardization”. NIST Information Technology Laboratory, Computer Security Resource Center. 2022. Available online: https://csrc.nist.gov/projects/ post-quantum-cryptography/post-quantum-cryptography-standardization

[46] National Security Agency. “Post-Quantum Cybersecurity Resources”. National Security Agency/Central Security Service. Available online: https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/

[47] M. Korolov, D. Drinkwater. “What is quantum cryptography? It’s no silver bullet but could improve security”. Apr. 6, 2020. Available online: https://www.csoonline.com/article/3235970/what-is-quantumcryptography-it-s- no-silver bullet-but-could-improve-security.htm

[48] Atlantic Council. “Emerging Technologies: New Challenges to Global Stability”. Research Report, Scowcroft Center for Strategy and Security. May 2020. Available online: https://www.jstor.org/stable/resrep26000

[49] Executive Office of the President of the United States. “National Strategic Overview for Quantum Information Science”. Subcommittee on Quantum Information Science of the National Science & Technology Council. Sep. 2018.

[50] M. C. Libicki, D. Gompert. "Quantum Communication for Post-Pandemic Cybersecurity". NATO’s 13th International Conference on Cyber Conflict (CyCon), 2021, pp. 371-386, Tallin, Estonia. doi: 10.23919/CyCon 51939.2021.9468295

[51] Council of Europe. “Budapest Convention Treaty No. 185: Convention on Cybercrime, Council of Europe”. Nov. 23,2001.https://www.coe.int/en/web/cybercrime/the-budapest-convention,https://www.coe.int/en/web/ conventions/full-list/-/conventions/ treaty/185

[52] North Atlantic Treaty Organization (NATO). “Cyber-Attacks Can Reach a Threshold That Threatens National and Euro-Atlantic Prosperity, Security, and Stability. Their impact could be as harmful to modern societies as a conventional attack”. Wales Summit Declaration. Sep. 5, 2015. Available online: https://www.nato.int/cps/ic/natohq/official_texts_112964.htm

[53] T. Vance, O. Bulda, A. Vance. “International Law in Cyberspace: The Need for Collaboration and Coordination to Promote International Peace in the Fifth Domain”. Journal of Cybersecurity Awareness and Education, Vol. 2 No. 1, 2020 and in the proceedings of Ninth Annual Cambridge International Law Conference on International Law and Global Risks: Current Challenges in Theory and Practice, University of Cambridge. United Kingdom. Available online: https://www.researchgate.net/publication/358833124_ International_Law_in_Cyberspace_The_Need_for_Collaboration_and_ Coordination_to_Promote_International_Peace_in_the_Fifth_Domain

[54] North Atlantic Treaty Organization (NATO). “Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare”. Tallinn Manual 2.0, supra note 70, at 12. Available online: https://ccdcoe.org/research/tallinn-manual/

[55] Executive Office of the President of the United States. “The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force”. The White House, Press Release. Jun 10, 2021. Available online: https://www.whitehouse.gov/ostp/news-updates/2021/06/10/the-biden-administration-launches-the-national-artificial-intelligence-research-resource-task-force/

[56] Department of Homeland Security. “DHS Releases Guidance to Mitigate Security Risks with the Advancement of Quantum Computing”. Press Release, Homeland Security. Oct. 4, 2021. Available online: https://www.dhs.gov/news/2021/10/04/dhs-releases-guidance-mitigate-security-risks-advancement-quantum-computing

[57] J. Mattila, K. Mäkäräinen, M. Pajarinen, et al. “Quantum Computing is Coming: Will Cybersecurity be Compromised?”. Digibarometer, The Status of Cybersecurity in Finland. pp. 41- 44. Helsinki. 2022. Available online: https://www.etla.fi/en/latest/quantum-computing-is-coming-will-cybersecurity-be-compromised/

[58] M. Nahed, S. Alaweh. “Cybersecurity in a Post-Quantum World: How Quantum Computing Will Forever Change the World of Cybersecurity”. American Journal of Electrical and Computer Engineering. Vol. 4(2): pp. 81-93. Jun. 2022. doi: 10.11648/j.ajece.20200402.17 ISSN: 2640-0480. Available online: http://www.sciencepublishinggroup.com/j/ajece

[59] United States Congress. “United States Code, Chapter 39, Arms Export Control, Subchapter I, Foreign and National Security Policy Objectives and Restraints. Title 22, Foreign Relations, and Intercourse. Available online: https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter39&edition=prelim