Scientific Research Publishing

Journal of Quantum Information Science, 2023, 13, 56-77
https://www.scirp.org/journal/jqis
ISSN Online: 2162-576X
ISSN Print: 2162-5751

Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges

Sabina Sokol

Girls in Quantum, CA, USA
Email: sabinaeinatsokol@gmail.com

How to cite this paper: Sokol, S. (2023) Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges. *Journal of Quantum Information Science*, **13**, 56-77.
https://doi.org/10.4236/jqis.2023.132005

Received: May 20, 2023
Accepted: June 27, 2023
Published: June 30, 2023

Abstract

This research paper analyzes the urgent topic of quantum cybersecurity and the current federal quantum-cyber landscape. Quantum-safe implementations within existing and future Internet of Things infrastructure are discussed, along with quantum vulnerabilities in public key infrastructure and symmetric cryptographic algorithms. Other relevant non-encryption-specific areas within cybersecurity are similarly raised. The evolution and expansion of cyberwarfare as well as new developments in cyber defense beyond post-quantum cryptography and quantum key distribution are subsequently explored, with an emphasis on public and private sector awareness and vigilance in maintaining strong security posture.

Keywords

Quantum Computing, Post-Quantum Cryptography (PQC), Quantum Hacking, Cybersecurity, Internet of Things (IoT), Shor's Algorithm, Quantum Random Number Generators (QRNGs), Pseudorandom Number Generators (RNGs), Quantum Key Distribution (QKD), Symmetric Key Cryptography, Asymmetric Key Cryptography

1. Introduction

Since the moment Peter Shor first proposed his famous algorithm in 1994—which has been mathematically proven to break some modern cryptographic standards—the international community has raced to build the first cryptanalytically relevant quantum computer (CRQC) that can apply it. The recent surge of new quantum companies and research groups has raised the prospect of developing such a technology closer, with experts predicting that a CRQC will be available—though likely not commercially—in the next five to seven years [1].

Asymmetric cryptographic algorithms—those that use a combination of pub-

lic and private keys to encrypt data, such as Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie-Hellman—will be highly vulnerable to attacks by these devices. These schemas are designed around difficult mathematical problems—such as large prime number factorization—for which there are no efficient classical algorithmic solutions. Moreover, the principle of "Harvest Now, Decrypt Later"—the phenomenon of stealing encrypted, highly confidential data with the intent of later decrypting it with a CRQC—asserts that it ultimately does not matter when such a technology will be developed because the information possessed by adversaries—such as personal health records—will still be socially, politically, or economically damaging. Therefore, it is critical that the public and private sectors migrate towards post-quantum cryptography (PQC)—a class of CRQC-resistant algorithms designed to be implemented on classical computers—as soon as possible. The process of transitioning to these new standards will take many years depending on the size and complexity of the agency. As a result, industry experts and government officials urge starting the process now to protect sensitive data. Regulators in several western countries have released requirements or recommendations urging organizations to commence the migration process immediately. However, PQC migration should not be the only area of concern regarding the threat quantum poses to national and international security. One should go beyond current corporate trends and media hysteria to understand the rest of the picture. Doing so will reveal the vast landscape of largely unaddressed concerns within the quantum cybersecurity space, all of which may have a significant impact on digital privacy and integrity in the near future.

2. The Current Federal Quantum/Cyber Landscape

In October 2020, the National Security Agency (NSA) released a statement giving a high-level overview of quantum key distribution (QKD)—quantum-secure communication protocols that harness properties of quantum mechanics to ensure the confidentiality and integrity of data being transmitted—and quantum cryptography. It outlined the limitations of the former technology, namely the incredibly high cost of implementation [2]. The agency declared that it will not support QKD's usage for national security systems (NSS) and will not invest in certifying QKD products in the near future [2].

In March 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released a statement outlining the four main areas of focus for cyber resiliency and defense, which include transportation systems, election security, critical supply chains, and ransomware protections [1]. The agency emphasized that cyber attacks are inevitable, referencing the major data breach at the federal level in 2019-2020: a state-sponsored group compromised several hundred organizations worldwide, both in the public and private sectors, exposing millions of customers' personal information. CISA also instructed federal agencies to inventory all cryptologic systems, infrastructure, security standards, and critical

data that will need to be updated once the official post-quantum cryptographic standards are released by the National Institute of Standards and Technology (NIST) [1]. Additionally, the statement emphasized the much-needed focus on Diversity, Equity, Inclusion, and Accessibility (DEIA) in the cyber workforce, foreshadowing the Department of Defense's (DoD) release of the 2023-2027 Cyber Workforce Strategy two years later.

In May 2022, the White House released a national security memorandum outlining the threat of CRQCs to military and civilian infrastructure [3]. It called for further quantum information science (QIS) education, research, and workforce development. It also stated that all corporations and agencies working in the field of quantum should establish a liaison with the Office of Science and Technology Policy (OSTP) by August 2022 to begin the transition to quantum-resistant cryptography immediately [3]. NIST announced the establishment of a working group for NSS owners to ensure all further guidance on PQC meets industry needs. The agency also mandated that all Federal Civilian Executive Branch (FCEB) agencies should report on all systems that are vulnerable to CRQCs to CISA by May 2023; funding for the migration to PQC will be evaluated accordingly. On the same note, NSA, NIST, and other security agencies confirmed the release of official PQC migration guidelines to NSS customers by May 2023 as well [3].

In June 2022, NIST announced the first four quantum-resistant algorithms: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ [4].

In August 2022, CISA released guidelines for PQC preparation and migration primarily for NSS customers [5]. However, it recommended that all organizations with critical infrastructure follow the PQC roadmap, which highlights everything discussed in the March 2021 statement. The agency also emphasized that quantum computing poses a substantial threat to 55 national critical functions (NCFs) [5].

In September 2022, as an extension of the national security memorandum released in May 2022, the NSA announced that NSS customers are to start migrating towards approved quantum-resistant algorithms—CRYSTALS-Kyber and CRYSTALS-Dilithium—immediately [6]. The agency expects to fully use these algorithms by 2035. However, it is requiring all NSS services, equipment, and operating systems to initially support CSNA 2.0 by 2025-2030, and shift to exclusive use of CSNA 2.0 by 2030-2033 [6]. This means that any NSS systems that use the CSNA 1.0 algorithms should either be removed or brought up to compliance. Currently, SHA-384, SHA-512, and AES-256 still stand as symmetric cryptographic algorithms—those that use a single encryption key for two-party exchanges—for CSNA 2.0. The NSA also declared that it should approve any and all deviations from complete CSNA 2.0 implementation for NSS systems [6].

In November of 2022, the White House sent out its own extension to the May memorandum directed for non-NSS. The Office of Management and Budget (OMB) called for agencies to inventory all information systems and technologies

that are vulnerable to CRQC-based attacks, starting with those that handle the most sensitive information [7]. The memorandum also required all agencies to designate someone to head this PQC migration initiative. OMB's statement assured FCEBs that CISA and the NSA will provide more guidance on next steps in the PQC process by February 2023, including guidance for PQC testing [7]. Lastly, the memo announced the establishment of another working group—headed by OMB—for agency representatives that deal with non-NSS.

In December 2022, NIST held its 4th PQC standardization conference, during which the finalists—Classic McEliece, BIKE, HQC, and SIKE—were presented [8]. The organization also declared that it is planning to standardize the Round 3 finalists: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON [8]. It also announced that the first official PQC standards will be published in early 2024, but called for new submissions for non-lattice-based digital signature schemes—methods of ensuring a message's authenticity and integrity—by June 2023. The National Cybersecurity Center of Excellence (NCCoE) underscored the fact that most organizations lack a firm understanding of the cryptographic standards currently employed in their information technology (IT), stating this as the primary reason for immediate PQC migration efforts [8].

A week later, the White House held the National Quantum Initiative (NQI) Centers Summit, emphasizing DEIA in the QIS and greater STEM workforce. The idea of a "quantum-smart"/"quantum-capable" society was raised, establishing a long-term goal for teachers, students, and families to be knowledgeable about and comfortable working with quantum technologies [9]. President Biden then appointed the 15-person National Quantum Initiative Advisory Committee (NQIAC) to advise his cabinet and Congress about the latest NQI developments, specifically in QIS [9].

At the end of December 2022, President Biden signed the "Quantum Computing Cybersecurity Preparedness Act" into law, raising the urgency for PQC migration of federal IT, excluding NSS [10]. The act assured agencies that OMB would issue guidance about an IT inventorying process akin to CISA's framework in March 2021. It also confirmed that OMB will oversee all PQC migration communication with CISA and Congress, as well as PQC testing and IT risk assessments following NIST's release of the 2024 guidance [10].

In March 2023, the Biden-Harris administration released the latest "National Cybersecurity Strategy," outlining their mission to strengthen cyber defense by defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future, and forging international partnerships to pursue shared goals [11]. The federal government pledged to continue investing in quantum computing and security research and education, citing its May 2022 memorandum to re-emphasize the urgency of PQC migration for public networks and systems [11].

3. The Internet of Things

In the era of Web 3.0—the third generation of Internet innovation, characterized

by ubiquitous computing across decentralized networks such that users have greater control over their data—cybersecurity has become more critical than ever before. With over fifteen billion Internet of Things (IoT) devices—physical objects such as thermostats and refrigerators that connect to and send data over the Internet—constantly collecting and processing user information, the threat of data leakage and exploitation is now too high [12]. Because IoT hardware is typically compacted into very small objects, it often has very limited energy and data storage banks. Thus, unlike most standard-sized machines, these devices physically cannot employ resource-intensive cryptographic schemas to ensure the highest level of information security possible. As such, it can be reasonably inferred that most if not all PQC algorithms being currently tested simply exceed current IoT processing capabilities, making PQC migration unviable for this entire class of pervasive technologies.

Just as lighter-weight classical cryptographic schemas have been devised and implemented to ensure an acceptable level of IoT security, a similar class of PQC algorithms should be developed as well. Unfortunately, there has been no federal guidance specifically for IoT vendors on this matter, indicating a lack of strong public-private communication channels as well as urgency in addressing *all* quantum-impacted areas. This is a concern because PQC migration for IoT technologies is already predicted to take longer than standard device migration because of the sheer quantity and variety of products on the market. Moreover, many are single-use machines designed with custom operating systems and firmware, which further complicates the task of developing universal schemas.

To address this, NIST and other agencies overseeing this quantum shift should establish methods of keeping IoT vendors apprised of the latest—particularly light-weight—PQC developments and provide strict guidelines on their implementation. Inaccurate, incomplete, and simple lack of proper security configurations is already a widespread issue within the classical cybersecurity space because products are so diverse and the demands for the maximum, most simple end-user experience are so high. This issue will only be exacerbated by quantum, and should be addressed specifically within the IoT sector as it continues to grow exponentially in the coming years. An industry feedback mechanism should also be established to facilitate more effective collaboration with PQC governance bodies so that future recommendations better align with vendors' needs. Similarly, the private sector should prioritize research into quantum-safe options and start preparing for hardware and software updates and upgrades to comply with new standards.

IoT maintenance is also a widespread issue, with many users leaving device software non-updated for years, allowing the number of exploitable—but avoidable—vulnerabilities accumulate, which significantly increases the risk of cyber attacks and personally identifiable information (PII) breaches [13]. It can be reasonably assumed that this concern will only grow as the threat of CRQCs looms closer. Thus, even if all 400+ current IoT vendors make a collective effort with the federal quantum guidance body to develop and implement light-weight PQC

algorithms in a timely manner, the likelihood that more than a small fraction of those devices will indeed be fully upgraded to meet quantum-safe standards is extremely low [14]. Hence, the IoT quantum security discussion should also include measures of better ensuring user compliance to PQC standards. It is indeed evident that a large-scale effort is needed to bring the billions of soon-to-be "legacy" devices—ones that are critically outdated—up to par. The cost of *not* doing so will be at least in the range of hundreds of billions of dollars [15].

4. The Public Key Infrastructure

It has been widely documented that asymmetric cryptographic schema—most notably RSA, ECC, and Diffie-Hellman—can and will be broken by the aforementioned Shor's algorithm. However, it is important to note that other aspects of public key infrastructure (PKI)—which employs asymmetric schema to maintain the confidentiality and integrity of Internet communications using a structure of certificate-based trust relationships—may be vulnerable to quantum attacks as well. In particular, most secure Internet protocols may be at risk. These include Transport Layer Security (TLS), which is used to secure web traffic as part of Hypertext Transfer Protocol Secure (HTTPS); Secure Shell (SSH), which is a secure communication protocol used for network operations and remote computer management; and Pretty Good Privacy (PGP/OpenPGP), which is primarily used to secure email communication [16]. These hybrid cryptosystems leverage asymmetric standards—namely RSA and Diffie-Hellman—in combination with symmetric standards—namely Blowfish, Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) for more secure and efficient encryption.

Most quantum security researchers agree that symmetric cryptography is currently not as vulnerable to quantum attacks as its asymmetric counterpart is [17] [18]; however, the hybrid models discussed still need to be revised and/or replaced because of the asymmetric attack surface. NIST and other bodies including the Institute of Electrical and Electronics Engineers (IEEE) as well as the Quantum Security Alliance (QSA) are currently analyzing and testing PQC algorithms, but have not released any formal communication regarding how these will then be integrated with the rest of PKI. While OpenSSL, OpenSSH, and some other collaborative open-source task forces have begun proactively prototyping quantum-safe schemas, unfortunately, most public and private entities have decided to remain passive on post-quantum mitigation and migration [19] [20].

Cloud computing—the practice of utilizing resources and processing power on demand via the Internet without direct management of these capabilities—has emerged as a key method of increasing availability to and reducing costs of infrastructure, platform, and software requirements [21]. In the era of Everything-as-a-service (E/XaaS) where even PKI deployments have moved off premises, it is critical to retain cyber resiliency, especially with such heavy re-

liance on a single or handful of providers to satisfy a broad spectrum of service needs. The cloud model is unfortunately not inherently quantum-resistant as it too relies on hybrid cryptosystems, whose vulnerabilities—as discussed previously—are too prevalent to ignore.

Fully homomorphic encryption (FHE)—which utilizes the fact that it is very difficult to calculate the distance data is from a point in a lattice—offers a practical solution [22] [23]. This classically- and quantum-safe schema allows for encrypted data to be utilized and processed without first decrypting it, thereby preserving confidentiality and integrity at the highest level [24]. Such a leakage-resistant technology—one that is not susceptible to side-channel attacks in which a malicious actor exploits design flaws in the physical system—can be leveraged specifically in cloud computing [22]. Providers and other third parties can safely operate on outsourced, private information without requiring access to or the possession of the secret key, which is largely impossible with other cryptographic standards where operations can only be performed once data is decrypted.

While FHE is yet to be standardized due its inefficiency and large storage requirements, it has great potential for implementation as a secure, quantum resistant algorithm in the near future. The Homomorphic Encryption Standardization Consortium led by global government, industry, and academia leaders—including the NIST, the entity overseeing the PQC standardization conference—has made recent strides in the optimization of this schema, suggesting the realization of real-world applications in the near future [25]. The widespread dependency on cloud technologies will likely be supported by this new security model, with data privacy and client-provider trust at its core.

5. The Symmetric

The quantum impact on symmetric cryptography is substantially less significant than that on asymmetric cryptography, namely because attack vectors like Grover's algorithm—which offers a polynomial speedup for unstructured search problems—are currently too time and resource intensive to substantially threaten private-key exchanges, under the condition that key sizes are at least doubled [16]. However, this recommendation should still be taken seriously and implemented quickly, as organizational IT and cyber departments may be susceptible to leaving their security configurations on now-vulnerable, default standards.

Psychologically speaking, humans generally avoid unnecessary decision making, commonly characterized by leaving default settings—whether for organ donor registration or web account creation—as they are [26]. This principle of nudge theory—the concept of influencing individuals' behavior and decision-making—can and should be applied to aid global quantum-safe cryptography efforts by standardizing and mandating the removal of insecure options from hardware and software products, if possible. In practice, consumers within the public and private sectors will be automatically more secure, as the path of

least resistance will support the updated security guidelines. Regardless of implementation procedures, the time and resource costs associated with this shift to larger key sizes should be evaluated and planned accordingly with hardware and software capacity constraints in mind, as longer schemas require longer data processing times.

However, consistently doubling key sizes will not be viable in the long-term. Artificial intelligence (AI)—machine intelligence that harnesses computer science and data analysis to solve complex problems—has and will inevitably continue to accelerate quantum computing, which in turn will accelerate AI, thus creating a virtuous cycle of endless exponential growth across both fields. As such, all current PQC algorithms—as standardized by NIST—will likely be broken at some point; a continuous evolution of these solutions will be required, along with a standardized process for phasing out and replacing the freshly insecure ones. This synergy of AI and quantum will be harnessed to successfully implement Grover's—among others, as algorithm development will also be accelerated—within the next couple decades, a direct threat to current symmetric cryptographic schema. Therefore, revisions and/or replacements to existing algorithms should be developed in the near future.

Aside from the principle of doubling private keys, it has become apparent that the integrity of the exchanges themselves can no longer be guaranteed with the application of Simon's algorithm—a precursor to Shor's algorithm. Message Authentication Codes (MACs)—which serve as checksums for message digests to ensure that data has not been intentionally or unintentionally modified in transit—are widely used with SSL/TLS and are constructed from block ciphers—those that encrypt data in specific chunk sizes [27] [28]. Moreover, they are often integrated in Authenticated Encryption with Added Data (AEAD) algorithms, which bind additional, variable data to encrypted messages, preventing adversaries from "replaying" ciphers that were previously sent during a communication session. Unfortunately, the prospect of using Simon's to break most MAC and AEAD schema is substantially high, especially because newer, more robust modes are commonly constructed from deprecated ones, which are not quantum-secure [29]. Most notably, Cipher Block Chaining Message Authentication Code (CBC-MAC), Cipher Block Chaining Hash-Based Message Authentication Code (CBC-HMAC), Offset Codebook Mode (OCB), and Advanced Encryption Standard Galois/Counter Mode (AES-GCM) have all been deemed breakable [17] [29] [30]. Thus, the development of new integrity-ensuring mechanisms for symmetric-reliant systems is critical in ensuring longer-term security.

6. The Other

Beyond assessing high-level cryptographic algorithms for quantum vulnerabilities, one should examine the more primitive technologies embedded within secure systems. Debates on the efficacy of pseudo-random number generators (PRNGs)—deterministic algorithms that generate sequences of quasi-random

numbers using initial values—in a post-quantum era have recently surfaced [31] [32]. Quantum-random number generators (QRNGs)—in deterministic algorithms that harness specific principles of quantum mechanics to generate sequences of truly unpredictable random numbers—have also garnered a significant amount of attention because of their use in QKD [32]. They are classified as true random number generators (TRNGs)—algorithms that leverage natural randomness, such as in variations in background radiation, to generate random sequences of numbers. While there are non-quantum-based TRNGs, many cryptography experts argue that these algorithms are not certifiably random because it is unclear whether the phenomena they exploit would be impossible to model in the future with more advanced technology. Therefore, this branch has similarly been under scrutiny by quantum researchers over whether they are vulnerable to quantum attacks. Both PRNGs and TRNGs are widely used in cryptographic key generation, digital signing, initialization values, security pins, and salts—additional, random strings of information added to passwords for added security. The consequences of breaking these critical algorithms would thus be devastating.

Some researchers have argued that PRNGs are just as effective as QRNGs particularly in machine learning methods, generalizing that the former is thus no less secure than the latter within cryptographic applications [33]. However, they do note that the outputs of both algorithms are explicitly differentiable, which raises a concern of whether one could accurately determine the class of RNG being used [33]. If evidence of a QRNG is detected, for example, one can affirm the existence of quantum nodes on a network. Such information would be highly valuable to an adversary who could tailor their attack strategy to exploit specific quantum or classical system vulnerabilities.

Other researchers have demonstrated that sub-classes of PRNGs currently employed in public and private infrastructure—namely the Blum-Micali family—can be broken with a variation of Grover's and Shor's algorithms combined [32], [34]. The subsequent conclusion that cryptographic systems are also vulnerable to this new set of attack vectors—namely compromised identity authentication and password confidentially mechanisms—is alarming, particularly because there has not been any federal quantum-oriented guidance on this matter. Just as agencies are being implored to establish inventories of their vulnerable asymmetric cryptographic systems, they should similarly analyze the use of P/TRNGs in their infrastructure. While PQC migration would address concerns over P/TRNGs used in key and digital signature generation, the other areas discussed should not be overlooked.

Though QRNGs have been established as highly attack-resistant because it is theoretically impossible to predict the random sequences they generate, implementing them is quite costly. Significant research and development of smaller, faster models has yet to be conducted. However, the European Union (EU) will likely lead this effort in the near future as this technology is a critical part of QKD, which is one of the countries' primary technological investments in prep-

aration for the post-quantum era [35] [36]. Alternatively, the United States (US) has directed its attention towards the development of PQC, so the extent to which the federal government will allocate resources towards QRNGs or more secure P/TRNGs remains unclear [2]. These vastly different approaches to quantum cybersecurity shall be analyzed and compared as the advent of CRQCs grows ever-closer.

7. The Race

Dozens of countries from all around the world are currently investing billions of dollars into QIS research, furthering quantum computing innovation, and harnessing applications for quantum technologies across industries from finance to drug discovery. It is critical that the US remain at the forefront of such developments, as highlighted in National Security Memorandum 10 and implied in the 2023 National Cybersecurity Strategy. While the incoming quantum revolution is expected to usher in a new era of technological and social progress marked by rapid optimization and innovation across the public and private sectors, threat actors ranging from terrorist groups to nation states have been eyeing this trend as an opportunity to launch devastating attacks with incredibly large payouts. The prospect of widespread attacks on US critical infrastructure—such as power grids—is well within reach as evidenced by Russia's history of such schemes on Ukraine, among other nations [37].

Cyber warfare has been rising at an alarming rate over the past few decades, with both the US and its greatest enemies—including but not limited to Iran, North Korea, and Russia—rigorously attempting to compromise each other's abilities to flourish economically [37]. The lack of international guidance surrounding this global issue is already deeply troubling and will only be exacerbated with the continuous advancement of emerging technologies. Just as world powers were initially reluctant to establish policies limiting and then prohibiting the use of chemical warfare following the world wars because it subsequently hindered their own ability to use the weaponry, one can infer that current leaders—including those within the US—are hesitant about taking similar steps in this digital age [38]. Offensive and defensive quantum-cyber strategies and laws should be developed and coordinated across the international community to ensure the security of civilians, industries, and infrastructure. Failing to do so may allow a number of unprecedented attacks to wreak havoc on society.

Moreover, effective emergency response on all levels to those attacks cannot be developed and maintained without a dynamic collective understanding of what the threats are in the first place. Just as a fire department builds its incident command system (ICS) protocols off of baselines surrounding known fire behaviors and patterns, intelligence agencies should similarly continue to track potentially dangerous or suspicious activity and communicate as much of that information to corporations, critical infrastructure authorities, and ordinary users as possible. The challenge of collaborating with foreign entities while remaining

wary of attempts to undermine or exploit domestic systems—as well as maintaining an open dialogue with the general public while staying cautious of insider threats—is significant. However, greater transparency and cooperation are vital to protecting social, economic, and political order worldwide. The effort to facilitate this—particularly surrounding cyberwarfare defense and policy—should continue to grow.

8. The Defense

Beyond the PQC dialogue, several nations have invested heavily into other areas of quantum cybersecurity, most notably harnessing the power of quantum neural networks (QNNs)—quantum-classical models inspired by the construction of the human brain that perform complex processes, such as image recognition [39]. This technology has been implemented in next-generational intrusion detection systems (IDSs)—hardware or software packages used to monitor network traffic for abnormal and malicious behavior [40]. As cyber attacks have become further automated and more pervasive with AI enhancements, the need for effective IDS solutions—particularly for large enterprises that manage tens of thousands of devices simultaneously—has risen significantly.

The use of QNNs for faster, more robust pattern recognition allows for greater visibility across infrastructure as well as quicker incident response times. China's cyber mimic defense (CMD) system, for example, employs QNNs in a polymorphic solution that dynamically adapts to hostilities by concealing and manipulating a network's external—Internet-facing—appearance [40]. Such a strategy has been demonstrated to effectively defend against millions of simultaneous network attacks, as evidenced by the 24-hour global white-hat competition several years ago, during which China gave thousands of cybersecurity researchers and enthusiasts free reign to pummel a network using the CMD system in an attempt to bring it down [40]. The use of QNNs to maintain such resiliency is quite impressive, and its applications should be explored by the US government as well; the technology may be a viable mechanism for protecting highly sensitive infrastructure beyond PQC, the area that has been dominating the post-quantum preparation conversation for the past several years.

Quantum computing has thus proven to be a vehicle of both cyber offense and defense within the international community. Heavy investment in the latter area—beyond cryptography—is necessary for the US to retain its lead in this emerging technology field. Allies and adversaries alike do not only concern themselves with the confidentiality and integrity of communications and critical assets ensured by strong encryption standards. The majority of cyber attacks are not perpetuated on these schemas in the first place [41]!

Resiliency requires holistic analysis and implementation of quantum-enhanced technologies across attack surfaces, rather than hyper-focus on a smaller subset of vulnerabilities. The development of these mechanisms is analogous to the use of unified threat management (UTM) platforms—hardware or software pack-

ages that address a wide variety of security necessities. Ideally, one would deploy separate devices that are each highly adept at mitigating each class of threats, but in cases where the capacity to do so is limited, one settles for just one device that is decently capable of wholly addressing several classes of common threats. Because quantum is still nascent, highly effective mechanisms designed to mitigate specific, quantum-based cyber vulnerabilities have not been developed yet. Therefore, it is critical to invest significant time and resources into ensuring UTM-like, "basic coverage" across a wide range of these vulnerabilities before directing that attention towards narrower areas of concern, such as strictly asymmetric cryptography. Otherwise, a determined attacker could simply discard PQC-protected attack vectors and focus on the other areas described throughout this paper. Being ready for post-quantum means being cognizant of the broader cyber problem and actively addressing it by investing into a broader range of post-quantum defense mechanisms.

Several quantum researchers have advocated for a "shared service" model—where services are funded, resourced, and provisioned by a particular department in an organization—asserting that this approach will lessen the burden on individual entities who seek to implement the necessary quantum-resistant measures [42] [43]. Prioritizing collaboration and establishing interdependent relationships between the public and private sectors is therefore necessary to democratize access to relevant materials and tools. In particular, consolidating the varying levels of guidance and research surrounding quantum will better enable agencies and vendors to follow and implement the latest developments in quantum-resistant algorithms and other technologies faster. Further centralization in this area among the international community is also critical in leveraging the wide variety of ideas, strategies, and developments to only foster greater innovation and ensure greater "coverage" over a larger attack surface, benefiting all parties involved.

9. The Concern

In preparing for the next generation of quantum—and the new class of cybersecurity vulnerabilities that comes with it—it is important to analyze and subsequently strengthen approaches to addressing existing digital privacy and integrity challenges. Based on data compiled in early April 2023, there were over 236 million ransomware attacks worldwide in just the first six months of 2022, with businesses losing roughly $4.35 million per data breach that year [44]. The rate and severity of cybercrime overall has significantly increased in the past several years, with twenty percent of all Internet users globally—over one billion people—having had an alarming one billion email addresses compromised [44]. These issues will only be exacerbated by the incoming quantum technology revolution and should be dealt with more aggressively than ever before.

The lack of secure programming practices has similarly been a widespread issue in software and firmware development, with many companies prioritizing

rapid product releases over slower—but more hygienic—testing procedures. The 2023 Gartner report concluded that "90% of employees who admitted undertaking a range of unsecure actions during their work activities knew that their actions would increase risk to the organization and undertook the actions anyway," thereby emphasizing the rampant inadequacy of cybersecurity awareness [45]. As further underscored in the 2023 National Cybersecurity Strategy, there is currently a lack of legislation surrounding vendors' liability for failing to comply with secure development frameworks [46]. Further discussion and Congressional action on this issue is needed to incentivize the practice of secure-by-design principles and adequate pre-testing amidst heavy market competition. Financial resources should also be allocated towards properly educating current and future generations of developers and engineers on working with quantum-safe algorithms and protocols.

Quantum workforce development begins with K-12; younger generations will make up the future body of technology innovators and policymakers in this field. As such, current STEM education should be revised and restricted to better cultivate understanding of emerging technologies. However, due to the current lack of standardization across quantum computing, programming, algorithm development, and cryptography, there is no clear direction for getting involved in the field. With companies vying to attain quantum advantage—the point where a quantum computer can solve a problem faster and more efficiently than a classical computer—it has become increasingly overwhelming to discern a proper starting point, particularly one that does not require sifting through highly technical documentation. This decentralization then serves as a significant barrier for the dissemination of quantum-cyber hygiene principles, which is detrimental to post-quantum cybersecurity as humans continue to lie at the crux of threat mitigation [47]. In fact, the most common recommendation made by industry and government leaders for maintaining greater resiliency has been emphasizing user education through textbooks, workshops, and gamification [47]. However, it is evident these protocols are not enough to curb the alarming rate of data breaches and resultant expenses. Research shows that "current training programs … have no impact" on "users' cyber hygiene behaviors or knowledge" [48]. These existing solutions have leveraged extrinsic factors—such as money or status—to incentivize individuals to take more precautions surrounding their digital privacy and integrity, and fail to incorporate alternative mechanisms that may be more effective.

In exploring cognitive psychology and the literature surrounding behavioral change, it's become apparent the intersection between these areas and cybersecurity has yet to be thoroughly explored. Very little literature exists on harnessing intrinsic drive and other innate human factors to compel populations to truly invest in important public issues like digital safety. Governing bodies and industry leaders within the classical and quantum cybersecurity policy space should consider investing in the development and analysis of intrinsic models to improve civilians' knowledge and practices within both fields. These entities will

be responsible for executing solutions should they prove to be more effective than existing user training programs, which will require significant structural and procedural changes within organizations nationwide. While this process may seem daunting in the short-term, the cost of not investigating and implementing serious changes in classical cybercrime mitigation will result in a continuous surge of attacks—the consequences of which will continue to devastate individuals and small and large businesses alike—and subsequently exacerbate security challenges within the quantum space. Government agencies cannot disregard existing threats to digital privacy and integrity when developing comprehensive post-quantum defense frameworks because quantum computing and PQC will likely not be implemented ubiquitously. Rather, many hardware researchers and manufacturers are currently working to develop hybrid models—quantum and classical, together—for public and private use [49] [50]. A serious investment should therefore be made in the synthesis and centralization of quantum-cyber resources.

10. Conclusions

Evidently, there are many areas of quantum cybersecurity beyond asymmetric cryptography that should be discussed and addressed right now. The common fixation on PQC has left the IoT and cloud technology spaces; once relatively secure Internet structures; primitives of symmetric cryptosystems; several classes of RNGs; and the quantum workforce grasping for some attempt at navigating the looming post-quantum world. All entities invested in cultivating the new era of stronger digital privacy and integrity share the responsibility of building stronger public-private communication channels, encouraging collaboration between both domestic and international academic and industry spaces, standardizing and centralizing the roadmap for a safer post-quantum future, and cultivating a "quantum-smart" society.

Unfortunately, the majority of end-users, institutions, thought leaders, government officials, and policy makers are not properly educated nor vehemently concerned about the future of cybersecurity and their own cyber and physical safety. PII is not the only source of exploitation and long-term disruption to the global economy. Critical infrastructure—ranging from energy to healthcare to nuclear technologies—has been and will continue to be a prime target for state-sponsored adversaries that are determined to further undermine world powers [37]. The cost of not acknowledging and not adequately addressing this reality is too significant to ignore. In the meantime, a concise list of the proposed action items highlighted in this paper is provided below.

Proposed Action Items:

• Government entities should continue constructing and releasing post-quantum guidance in a timely manner such that it is readily available and highly readable by both vendors and consumers of technology products.

• NIST and other agencies overseeing large-scale post-quantum migration shift should establish methods of keeping IoT vendors apprised of the lat-

est—particularly light-weight—PQC developments and provide strict guidelines on their implementation.

• An industry feedback mechanism should be established to facilitate more effective communication with PQC governance bodies so that future recommendations better align with vendors' needs.

• The private sector should prioritize research into quantum-safe options and start preparing for hardware and software updates and upgrades to comply with new post-quantum standards.

• The principle of nudge theory—the principle of influencing individuals' behavior and decision-making—should be applied to aid global quantum-safe cryptography efforts by standardizing and mandating the removal of insecure options from hardware and software products, if possible.

• New schema—particularly MAC and AEAD—should be developed for symmetric-reliant systems to ensure longer-term security beyond doubling key sizes.

• In addition to establishing inventories of their vulnerable asymmetric cryptographic systems, agencies should similarly analyze the use of P/TRNGs in their infrastructure.

• Offensive and defensive quantum-cyber strategies and laws should be developed and coordinated across the international community to ensure the security of civilians, industries, and infrastructure.

• Intelligence agencies should continue to track potentially dangerous or suspicious activity and communicate as much of that information to corporations, critical infrastructure authorities, and ordinary users as possible.

• The effort to facilitate greater transparency and cooperation surrounding cyberwarfare defense and policy should continue to grow because it is vital to protecting social, economic, and political order worldwide.

• The US should prioritize holistic analysis and implementation of quantum-enhanced technologies across attack surfaces, rather than hyper-focus on a smaller subset of vulnerabilities.

• The international community should prioritize collaboration and the establishment of interdependent relationships between the public and private sectors to democratize access to relevant materials and tools via a "shared services" model.

• Entities should analyze and subsequently strengthen approaches to addressing existing digital privacy and integrity challenges.

• The federal government should incentivize the practice of secure-by-design principles and adequate pre-testing amidst heavy market competition.

• Financial resources should be allocated towards properly educating current and future generations of developers and engineers on working with quantum-safe algorithms and protocols.

• Governing bodies and industry leaders within the classical and quantum cybersecurity policy space should consider investing in the development and analysis of intrinsic models to improve civilians' knowledge and practices within

both fields.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] (2021) Post-Quantum Cryptography. Homeland Security. https://www.dhs.gov/quantum

[2] NSA/CSS (2020) Quantum Key Distribution (QKD) and Quantum Cryptography (QC). National Security Agency/Central Security Service. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[3] (2022) National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. Proclamation No. NSM-10 F.R. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

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

[5] (2022) Preparing Critical Infrastructure for Post-Quantum Cryptography. CISA Insights. https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf

[6] NSA Media Relations. (2022) NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems. NSA. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se

[7] (2022) Proclamation No. M-23-02 F.R. Executive Office of the President Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

[8] NIST (2022) Fourth PQC Standardization Conference. NIST. https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference

[9] (2022) Readout: National Quantum Initiative Centers Summit. The White House. https://www.whitehouse.gov/ostp/news-updates/2022/12/05/readout-national-quantum-initiative-centers-summit/

[10] (2022) Quantum Computing Cybersecurity Preparedness Act. Congress. https://www.congress.gov/bill/117th-congress/house-bill/7535/text

[11] (2023) FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[12] Statista (2022) Number of Internet of Things (IoT) Connected Devices Worldwide

from 2019 to 2021, with Forecasts from 2022 to 2030. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[13] Prakash, V., Xie, S. and Huang, D. Y. (2022) Software Update Practices on Smart Home IoT Devices. ArXiv. https://arxiv.org/pdf/2208.14367.pdf

[14] Nick, G. (2023) How Many IoT Devices Are There in 2023? Techjury. https://techjury.net/blog/how-many-iot-devices-are-there/#gref

[15] Statista (2018) Projected Market Revenue of the Internet of Things (IoT) and Analytics Worldwide from 2015 to 2021, by Segment. Statista. https://www.statista.com/statistics/913299/projected-global-revenue-of-the-internet-of-things-segment/

[16] Bogomolec, X., Underhill, J.G. and Kovac, S.A. (2019) Towards Post-Quantum Secure Symmetric Cryptography: A Mathematical Perspective. International Association for Cryptologic Research. https://eprint.iacr.org/2019/1208

[17] Krelina, M. (2021) Quantum Technology for Military Applications. *EPJ Quantum Technology*, **8**, Article No. 24. https://doi.org/10.1140/epjqt/s40507-021-00113-y

[18] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J.L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V.C., Vallone, G., Villoresi, P. and Wallden, P. (2020) Advances in Quantum Cryptography. *Advances in Optics and Photonics*, **12**, 1012-1036. https://doi.org/10.1364/AOP.361502

[19] Leyden, J. (2022) OpenSSH 9.0 Bakes in Post-Quantum Cryptography to Future Proof against Attacks. The Daily Swig. https://portswigger.net/daily-swig/openssh-9-0-bakes-in-post-quantum-cryptography-to-future-proof-against-attacks

[20] Easterbrook, K. and Paquin, C. (n.d.) Post-Quantum TLS. Microsoft. https://www.microsoft.com/en-us/research/project/post-quantum-tls/

[21] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing. Computer Security. NIST. https://doi.org/10.6028/NIST.SP.800-145 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[22] Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Helevi, S., Hoffstein, J., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Shahai, A. and Vaikuntanathan, V. (2018) Homomorphic Encryption Standard. http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf

[23] Will, M.A. and Ko, R.K.L. (2015) Chapter 5-A Guide to Homomorphic Encryption. In: *The Cloud Security Ecosystem*, Elsevier, Amsterdam, 101-127. https://doi.org/10.1016/B978-0-12-801595-7.00005-7

[24] Armknecht, F., Boyd, C., Carr, C., Gjosteen, K., Jaschke, A., Reuter, C.A. and Strand, M. (2015) A Guide to Fully Homomorphic Encryption. Cryptology ePrint Archive. https://eprint.iacr.org/2015/1192.pdf

[25] (n.d.) Homomorphic Encryption Standardization. https://homomorphicencryption.org/introduction/

[26] Van dalen, H.P. and Henkens, K. (2014) Comparing the Effects of Defaults in Organ Donation Systems. *Social Science & Medicine*, **106**, 137-142. https://doi.org/10.1016/j.socscimed.2014.01.052

[27] McGrew, D.A. (2008) An Interface and Algorithms for Authenticated Encryption. RFC. (Memo) https://www.rfc-editor.org/rfc/pdfrfc/rfc5116.txt.pdf https://doi.org/10.17487/rfc5116

[28] (2009) Chapter 3-An Introduction to Cryptography. In: Liu, D. and Author, L., Eds., *Next Generation SSH2 Implementation*, Elsevier, Amsterdam, 41-64. https://doi.org/10.1016/B978-1-59749-283-6.00003-9

[29] Santoli, T. and Schaffner, C. (2017) Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives. Rinton Press, Princeton. https://doi.org/10.26421/QIC17.1-2-4 https://dl.acm.org/doi/10.5555/3179483.3179487

[30] Takagi, T. (2016) Post-Quantum Cryptography. *Proceedings of 7th International Workshop* (PQCrypto 2016), Fukuoka, 24-26 February 2016, 3. https://link.springer.com/chapter/10.1007/978-3-319-29360-8_4#citeas

[31] Barker, E., Barker, W., Burr, W., Polk, W. and Smid, M. (2016) Recommendation for Key Management—Part 1: General. Revision 3, NIST. https://doi.org/10.6028/NIST.SP.800-57pt1r4 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf

[32] Guedes, E.B., De Assis, F.M. and Lula, B. (2012) Quantum Attacks on Pseudorandom Generators. *Mathematical Structures in Computer Science*, **23**, 608-634. https://doi.org/10.1017/S0960129512000825

[33] Bird, J.J., Ekárt, A. and Faria, D.R. (2019) On the Effects of Pseudorandom and Quantum-Random Number Generators in Soft Computing. *Soft Computing*, **24**, 9243-9256. https://doi.org/10.1007/s00500-019-04450-0

[34] Kelsey, J., Schneier, B., Wagner, D. and Hall, C. (1998) Cryptanalytic Attacks on Pseudorandom Number Generators. In: Vaudenay, S., Ed., *FSE* 1998: *Fast Software Encryption*, *Lecture Notes in Computer Science*, Vol. 1372, Springer, Berlin, 168-188. https://doi.org/10.1007/3-540-69710-1_12 https://www.schneier.com/wp-content/uploads/2017/10/paper-prngs.pdf

[35] European Commission (n.d.) The European Quantum Communication Infrastructure (EuroQCI) Initiative. European Commission. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[36] (2023) QKISS: Developing Ready-to-Deploy European Quantum Key Distribution (QKD) Systems. Photonics & Space. https://www.ixblue.com/north-america/qkiss-developing-ready-to-deploy-european-quantum-key-distribution-qkd-systems/

[37] Egloff, F.J. and Smeets, M. (2020) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's most Dangerous Hackers. *Journal of Cyber Policy*, **5**, 326-327. https://doi.org/10.1080/23738871.2020.1808032

[38] Gibney, A., Director. (2016) Zero Days. (Film) Magnolia Pictures. https://www.amazon.com/Zero-Days-Colonel-Gary-Brown/dp/B01I2C0UV6

[39] Qiskit (2023) Quantum Neural Networks. Qiskit. https://qiskit.org/documentation/machine-learning/tutorials/01_neural_networks.html

[40] Middleton, A. and Till, S. (2020) Quantum Information Processing Landscape 2020: Prospects for UK Defence and Security. DSTL. https://uknqt.ukri.org/wp-content/uploads/2021/10/Quantum-Information-Processing-Landscape-2020.pdf

[41] (n.d.) Cybersecurity: A Global Priority and Career Opportunity. University of North Georgia, Dahlonega. https://ung.edu/continuing-education/news-and-media/cybersecurity.php

[42] Johnson, J. (Host). (2023) ICYMI: The Race to Secure Federal Cryptographic Sys-

tems [Audio Podcast Episode]. In: Larsen, C. (Producer), The Buzz, ACT-IAC. https://www.actiac.org/buzz

[43] IBM (2021)Shared Services. IBM. https://www.ibm.com/docs/en/psww2500/2.3.2.0?topic=reference-shared-services

[44] Griffiths, C. (2023) The Latest 2023 Cyber Crime Statistics (updated April 2023). AAG. https://aag-it.com/the-latest-cyber-crime-statistics/

[45] Gopal, D., McMullen, L., Walls, A., Addiscott, R., Furtado, P., Porter, C., Isaka, O. and Winckless, C. (2023) Predicts 2023: Cybersecurity Industry Focuses on the Human Deal. Gartner. https://www.bitsight.com/thank-you/gartner-predicts-2023

[46] Jr Biden, J. and Harris, K. (2023) National Cybersecurity Strategy. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[47] Dortch, M. (2017) User Education for Cybersecurity: Yes, It's Worth It. invanti. https://www.ivanti.com/blog/user-education-cybersecurity-yes-worth

[48] Cain, A.A., Edwards, M.E. and Still, J.D. (2018) An Exploratory Study of Cyber Hygiene Behaviors and Knowledge. *Journal of Information Security and Applications*, **42**, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

[49] Hirayama, Y., Ishibashi, K. and Nemoto, K., Eds. (2021) Hybrid Quantum Systems. Springer Nature, Berlin. https://doi.org/10.1007/978-981-16-6679-7

[50] IONQ (2023) What Is Hybrid Quantum Computing. IONQ. https://ionq.com/resources/what-is-hybrid-quantum-computing

Appendix

AEAD: Authenticated Encryption with Additional Data—bind additional, variable data to encrypted messages, preventing adversaries from "replaying" ciphers that were previously sent during a communication session

AES: Advanced Cryptography Standard

AES-GCM: Advanced Encryption Standard Galois/Counter Mode

AI: Artificial Intelligence—machine intelligence that harnesses computer science and data analysis to solve complex problems

Asymmetric Cryptography: use a combination of public and private keys to encrypt data

CBC-HMAC: Cipher Block Chaining Hash-Based Message Authentication Code

CBC-MAC: Cipher Block Chaining Message Authentication Code

CISA: Cybersecurity and Infrastructure Security Agency—subset of DHS

Cloud Computing: the practice of utilizing resources and processing power on demand via the Internet without direct management of these capabilities

CMD: Cyber Mimic Defense—employs QNNs in a polymorphic solution that dynamically adapts to hostilities by concealing and manipulating a network's external, Internet-facing, appearance

CNSA 1.0: Commercial National Security Algorithm suite 1.0—most have been deemed non-quantum-resistant (legacy)

CNSA 2.0: Commercial National Security Algorithm suite 2.0—approved quantum-resistant algorithms

CRQC: Cryptanalytically Relevant Quantum Computer

DEIA: Diversity, Equity, Inclusion, and Accessibility

DHS: Department of Homeland Security

Digital Signing: a method of ensuring a message's authenticity and integrity

DoD: Department of Defense

ECC: Elliptic Curve Cryptography

EU: European Union

E/XaaS: Everything-as-a-service—a business model by which any form of computing, storage, network security, etc. can be outsourced to a cloud provider

FCEB: Federal Civilian Executive Branch

FHE: Fully Homomorphic Encryption—utilizes the fact that it is very difficult to calculate the distance data is from a point in a lattice

Grover's Algorithm: quantum algorithm that offers a polynomial speedup for unstructured search problems

HTTPS: Hypertext Transfer Protocol Secure—encrypted web communication protocol

Hybrid Cryptosystem: leverage asymmetric and symmetric cryptography for more secure and efficient encryption

ICS: Incident Command System—standardized organizational risk management structure

IDS: Intrusion Detection System—hardware or software packages used to monitor network traffic for abnormal and malicious behavior

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of Things—physical objects such as thermostats and refrigerators that connect to and send data over the Internet

IT: Information Technology—the use of networking devices, infrastructure, and processing to create, exchange, store, and secure electronic data

Leakage: the susceptibility to side-channel attacks in which a malicious actor exploits design flaws in the physical system

Legacy: critically outdated systems

MAC: Message Authentication Code—serves as a checksum for message digests to ensure that data has not been intentionally or unintentionally modified in transit

NCCoE: National Cybersecurity Center of Excellences

NCF: National Critical Function

NIST: National Institute of Standards and Technology

NQI: National Quantum Initiative

NQIAC: National Quantum Initiative Advisory Committee

NSA: National Security Agency

NSS: National Security Systems—any system involved in intelligence gathering or handling for military purposes, weapons systems, and the like

Nudge Theory: the concept of influencing individuals' behavior and decision-making

OCB: Offset Codebook Mode

OMB: Office of Management and Budget

OSTP: Office of Science and Technology Policy

PII: Personally Identifiable Information—any information by which an individual can be readily identified, directly or indirectly

PGP: Pretty Good Privacy—primarily used to secure email communication

PKI: Public Key Infrastructure—employs asymmetric schema to maintain the confidentiality and integrity of Internet communications using a structure of certificate-based trust relationships

PQC: Post-Quantum Cryptography—a class of quantum computer-resistant algorithms designed to be implemented on classical computers

PRNG: Pseudo-Random Number Generator—deterministic algorithms that generate sequences of quasi-random numbers using initial values

QIS: Quantum Information Science—the study of harnessing properties of quantum mechanics to circumvent current information and computer processing limitations of classical computers

QKD: Quantum Key Distribution—quantum-secure communication protocols that harness properties of quantum mechanics to ensure the confidentiality and integrity of data being transmitted

QNN: Quantum Neural Network—a quantum-classical model inspired by the construction of the human brain that is used to perform complex processes, such

as image recognition

QRNG: Quantum-Random Number Generator—an indeterministic algorithm that harnesses specific principles of quantum mechanics to generate sequences of truly unpredictable random numbers

QSA: Quantum Security Alliance

Quantum Advantage: the point where a quantum computer can solve a problem faster and more efficiently than a classical computer

RSA: Rivest-Shamir-Adleman

Simon's Algorithm: a precursor to Shor's algorithm

Shared Service: a service that is funded, resourced, and provisioned by a particular department in an organization

Shor's Algorithm: can break asymmetric cryptographic algorithms via rapid integer factorization

SSH: Secure Shell—a secure communication protocol used for network operations and remote computer management

STEM: Science, Technology, Engineering, and Math

Symmetric Cryptography: use a single encryption key for two-party exchanges

TLS: Transport Layer Security—most notably used to secure web traffic

TRNG: True Random Number Generator—an algorithm that leverages natural randomness, such as in variations in background radiation, to generate random sequences of numbers

US: United States

UTM: Unified Threat Management—hardware or software packages that address a wide variety of security necessities

Web 3.0: the third generation of Internet innovation, which is characterized by ubiquitous computing across decentralized networks such that users have greater control over their data

3DES: Triple Data Encryption Standard