Human-Centric
Cybersecurity
Partnership

QUANTUM READY CYBERSECURITY

UNDERSTANDING AND MANAGING THE RISK

JACQUELINE, CHAN
BEATRIZ, JEREZA
RACHAEL, MACHNEE
JANE, NGAN
SANJAMPREET, SINGH
DANE, VANDERKOOI

Human-Centric
Cybersecurity
Partnership

HUMAN-CENTRIC CYBERSECURITY REPORT PROJECT

The 2024 Human-Centric Cybersecurity Report Project brought together postgraduate students from across Canada and the United Kingdom to work with our partners from both private industry and the public sector to produce reports looking at the problem of ransomware through a transdisciplinary lens.

ABOUT HC2P

The Human-Centric Cybersecurity Partnership (HC2P) is a transdisciplinary group of scholars, government, industry and not-for-profit partners that generate research and mobilize knowledge that will help create a safer, more secure, more democratic and more inclusive digital society.

ACKNOWLEDGEMENTS

We would like to thank Accenture, Bell Canada, The Canadian Centre for Cyber Security (CCCS), Canadian Cyber Threat Exchange (CCTX), Desjardins, Field Effects, GoSecure, Innovation, Science and Economic Development Canada, The National Bank of Canada, The National Cybercrime Coordination Centre (NC3), Public Safety Canada, The Royal Canadian Mounted Police, Statistics Canada, The University of Montreal, and The University of Ottawa for their efforts in supporting this project.

Art by Michael Joyce

Cite as:

Chan, J., Jereza, B., Machnee, R., Ngan, J., Singh, S. & Vanderkooi, D. (2025) Quantum Ready Cybersecurity: Understanding and Managing the Risk. Human-Centric Cybersecurity Partnership HC2P. Dépôt légal, Bibliothèque et Archives nationales du Québec, 2025.,

ISBN: 978-1-7387249-7-0

The Human-Centric Cybersecurity Partnership is supported in part by funding from the Social Sciences and Humanities Research Council.

Social Sciences and Humanities Research Council of Canada

Conseil de recherches en sciences humaines du Canada

Canada

Contents

Quantum Ready Cybersecurity

UNDERSTANDING AND MANAGING THE RISK

Executive Summary

Quantum computing offers unparalleled computational power for the future, promising breakthroughs in fields ranging from drug discovery to complex data analytics. However, it also poses a grave current challenge to cybersecurity, as the threat that it poses in the future must be mitigated in advance. While it may be decades before a fully weaponized quantum computer emerges, adversaries can already harvest encrypted data now and decrypt it later, when quantum hardware matures. Consequently, governments and industry alike must take urgent measures to protect their online security.

In this report, we structure our analysis around three central research questions: How quantum computing will disrupt cybersecurity, how we can mitigate these threats, and how Canada should prepare for a post-quantum world. We leverage the perspective of seeking to understand the known-knowns, known-unknowns, and unknown-unknowns to categorize a spectrum of risks. Known-knowns

such as the vulnerability of RSA and Elliptic Curve encryption demand immediate adoption of post-quantum encryption (e.g., CRYSTALS-Kyber). Known-unknowns include the timing and scope of “harvest now, decrypt later” attacks, requiring continued research and cryptographic agility. Unknown-unknowns, such as the future interplay of quantum computing with AI and blockchain, indicate the need for long-term, interdisciplinary foresight.

Our recommendations address concrete pain points across policy, technology, and governance. (1) Accelerate the standardization of post-quantum encryption, with financial and logistical support for vulnerable groups like SMEs. (2) Expand funding for independent research, particularly on quantum’s societal impact and new attack vectors. (3) Introduce legislation (e.g., reforms to PIPEDA, Bill C-26, Bill C-27) and soft law mechanisms to ensure data protection and constitutionally compliant use of quantum decryption tools. (4) Launch broad-based education campaigns to improve cyber hygiene and promote digital inclusion. (5) Revamp risk management frameworks (beyond ISO-31000) to account for transdisciplinary, cascading threats. (6) Guide strategic assessments of supply chain dependencies — for instance, Canada’s critical minerals essential to quantum hardware. (7) Pursue international collaboration to set balanced export controls and prevent the weaponization of quantum technologies.

Finally, this report emphasizes that quantum readiness is not limited to any one sector or policy area. Critical infrastructure, healthcare, financial systems, IoT devices, and more all face interconnected vulnerabilities. By articulating the urgency and defining targeted steps—from legislative updates to educational initiatives—we offer a roadmap that is both pragmatic and inclusive. Meeting these challenges head-on will position Canada to foster a secure, equitable quantum ecosystem that upholds privacy and resilience in a rapidly evolving digital landscape.

> ***“The likelihood of a real quantum threat breaking public encryption is, in essence, a race against time.”***

1 Introduction

Despite there being no consensus on when we will see the arrival of early quantum computers for commercial applications, there is no time to waste in preparing for their arrival. Several nations have already launched quantum initiatives with the total global funding estimated to be around US$42 billion in early 2024 (McKinsey Digital, 2024). In Canada, the impact of quantum technology is expected to be diverse across governments, individuals, and industries, including the small and medium enterprises that contribute half of Canada’s GDP and most of its private-sector employment (Innovation, Science and Economic Development Canada [ISED], 2023) A number of countries, including Canada, have published quantum strategies, incorporating anticipated social and economic impact, and defensive and strategic postures (European Commission, 2016; Government of Canada, 2023; US Congress, 2018).

With modern nations embedding computing technology into every aspect of their operation, from e-government to e-commerce and IoT to smart wearables, it is clear that understanding the impact of quantum computing technology on cybersecurity is important to ensure that its introduction does not cause disruptions. With the aim of bettering that understanding and generating thoughtful discussion on this topic, we have created this report.

The report analyzes and synthesizes an array of academic and grey literature pertaining to the impact of quantum computer technology on cybersecurity. Furthermore, a diverse group of interdisciplinary cybersecurity experts were brought together to answer the following research questions:

1. How will quantum computing disrupt cybersecurity?
2. How to mitigate any associated cybersecurity threats?
3. How should Canada prepare for quantum computing?

The report begins with a technical overview of quantum computing, followed by an assessment of its impact on cybersecurity through societal, behavioural and regulatory perspectives. Due to the (pre) nascent nature of the technology, we have organized the discussion as follows:

- Known-knowns: these describe known risks, impacts and mitigation strategies that are established with a high degree of certainty
- Known-unknowns: these describe risks and mitigation strategies that have a high degree of uncertainty as to their impact.
- Unknown-unknowns: these describe unknown, conceptual or theoretical risks and their related solutions

The report then presents recommendations to support Canada's readiness to tackle cybersecurity risks in the quantum computing era.

2 Overview of Quantum Computing

Quantum computers are a highly anticipated innovation; they will allow us to solve problems that standard computers are either not complex enough to solve or would take too long to solve. This capacity comes from the greater complexity in how a quantum computer stores and processes information.

A standard computer stores information in units (or bits) of information being either a one or a zero. We might represent these bits as being a coin that is exclusively either a "1" or a "0". A quantum computer uses a quantum object called a qubit. These qubits can appear to be in two states at the same time (IBM, 2024), or that they can be held in superposition. When a qubit is in superposition, the information that it holds represents all the possible values of the qubit. (DelViscio, 2024). We might represent this as a coin with

Figure 1 - Binary bits vs. a qubit

two faces. On one side, it is a “1” and on the other it is a “0” (Oak Ridge National Laboratory, 2022). By flipping this coin but preventing it from landing, we are holding this coin in superposition, as while it flips, it represents an equal chance of landing on either side and consequently, we consider it to be both and every value in between.

When qubits are grouped, complex computational spaces are created, which can be used to solve problems that are too complex for standard computers. Standard computers combine their simple binary bits to perform operations (e.g., 0 + 0 = 0, 0 + 1 = 1, 1 + 1 = 1). Computational operations can be performed by combining complex qubits. We can represent our “qubit” coin while flipping as being either “1” or “0” at a constant frequency as a wave.

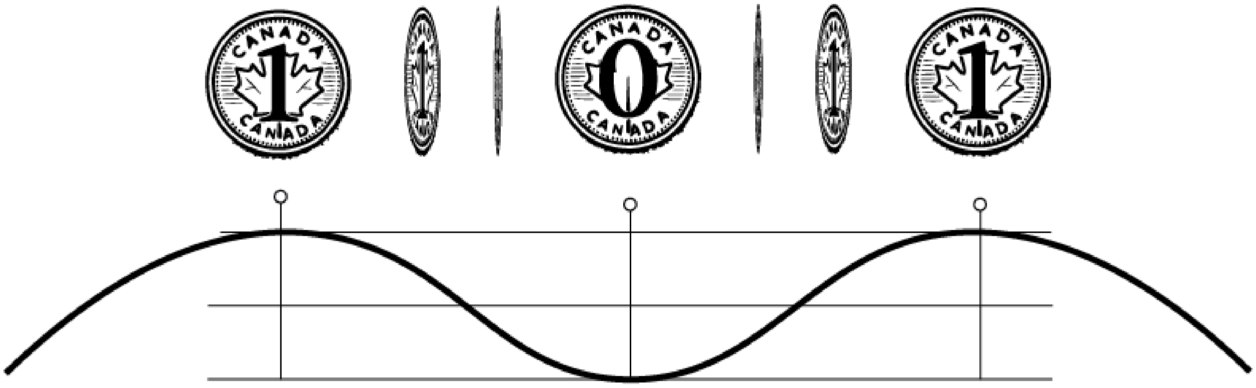

Figure 2 - A coin toss as a superposition of states

When qubits are combined, they can become entangled and, in this tangle, two qubits can become linked. When qubits are linked, a change to one will affect the other. Within clusters of entangled qubits in superposition interference will occur. This interference is similar to interference with waves. If we consider our coin’s wave at its peak at “1” and in a trough at “0”, linking it with another wave will have an impact.

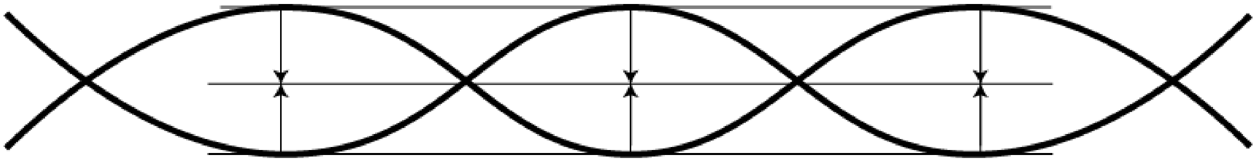

Figure 3 - Two waves linked destructively

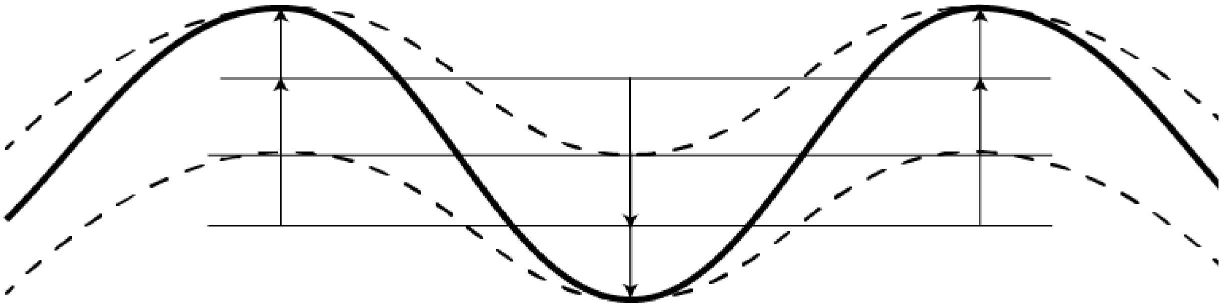

Figure 4 - Two waves linked constructively

If it is combined with a wave that is at an equal but opposite frequency, the peaks and troughs will destructively cancel each other out, resulting in no wave, or neither a “1” or “0”.

If it is combined with a wave that is at an equal and identical frequency, the peaks and troughs will constructively augment each other, resulting in a stronger “1” or “0”.

As the operation between the waves is not occurring at just the peak and the trough but at every point in between, it provides for more complexity than a binary operation, as there are theoretically an infinite number of points between the peaks and troughs that are interacting. Since the qubits are made up all of possibilities, the peaks and troughs represent the most probable answer. (IBM, 2024). Measuring the qubit will collapse its superposition (stop the coin from spinning), allowing it to be interpreted probabilistically as a classical result (e.g. ’1 or “0”) and be made useful.

3 Known Knowns

3.1 Breaking Encryption

There are well-established risks that quantum computing can pose to the cybersecurity landscape. It has now been widely accepted that an attack-capable quantum computer will break public key cryptography, which, in turn, can have serious implications for the information security landscape (Mashatan & Turetken, 2020). More precisely, quantum computing will be able to break many traditional and widely deployed encryption algorithms, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve cryptography (ECC) (Shor, 1994; Grover, 1996).

As Baseri et al., (2024) argues, the known and established risks of quantum computing can be classified into two groups: that affecting data at rest and that affecting data in transit. Data at rest refers to the capacity to disrupt encryption algorithms used for stored data, which is essential to modern security protocols and the ability to eliminate authenticity, integrity and non-repudiation of digital signatures. Data in transit refers to encryption of data as it moves between computers using network protocols such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec), which will be disrupted by quantum computing.

Despite the potential cybersecurity disruption posed by quantum computing, several mitigation strategies are already in place, depending on the specific operationalized schemes. For instance, a contemporary symmetric key encryption may be at risk of being broken via brute force via a quantum attack; however, the threat could be mitigated by swapping it to a post-quantum encryption algorithm or simply by increasing the key size to mitigate the threat (Zhang et al., 2023).

Transitioning infrastructure in preparation for a post-quantum world is already in progress. Larger corporations such as Apple have already deployed post-quantum encryption into their popular messaging service, iMessage (Apple, 2024). In addition, the National Institute for Standards and Technology (NIST) has begun updating their standards towards a post-quantum world. It has selected four “winners” of a post-quantum encryption development contest and established a deadline for standardizing these algorithms for 2024 (NIST, 2024). For general encryption, NIST has selected the CRYSTALS-Kyber algorithm, which boasts smaller encryption keys and faster speeds, enabling more cost-effective deployment and operational usage. For digital signatures where authentication, integrity and non-repudiation are most important, NIST has selected CRYSTALS-Dilithium, FALCON and SPHINCS+. The first two of these are similarly fast and efficient, like CRYSTALS-Kyber. SPHINCS+ despite being slower has the advantage of being mathematically distinct from the others, as it is hash-based, while the others are lattice-based.

Transitioning to quantum safe encryption may not affect everyone in the same way. Costs and logistical challenges associated with scaling and deployment may be lower for large firms relative to their general operating costs and who have access to capital pools and supporting resources. These costs and operational challenges are likely more of a barrier for smaller and medium sized enterprises. As in many cases the success of a protocol relies on its widespread adoption, this difference becomes an important factor. Unsurprisingly, the selection and deployment of quantum-resistant encryption at scale, whilst minimizing business costs and disruption, remains an unresolved question for policy-makers.

3.2 The Impact of Broken Encryption

3.2.1 Secure Communication (Emails, Messages, and Web Browsing)

Emails and messaging systems, such as encrypted emails using PGP and S/MIME, rely on public key cryptography to ensure that only the intended recipient can decrypt the message (R. Imam et al., 2021). Digital signatures verify the authenticity and integrity of the email sender, while web browsing via HTTPS uses public key infrastructure (PKI) and key exchange protocols (TLS/SSL) to secure data between a user’s browser and a web server. This ensures the confidentiality of sensitive information, such as login credentials and personal data (R. Imam et al., 2021). While the use of encryption for email might be less than desirable, they are widely used on messaging platforms and for web browsing (Reuter et al., 2021). Quantum computers, by potentially breaking the cryptographic algorithms, would allow attackers to decrypt what are likely to be sensitive emails and otherwise secure messages on currently private messaging services. They would also be able to intercept HTTPS connections to steal information leading to further harm. This is particularly concerning, considering the current trend towards the use of Software as a Service for critical business operations (Chai, 2022).

3.2.2 Digital Payments and Financial Transactions

Digital payments, including online banking transactions and those using Central Bank Digital Currencies (CBDCs) like Jura and Project Atom (Payments Canada, 2022), are secured using cryptography (Nili et al., 2024). Banking transactions rely on cryptographic protocols to ensure secure communications between users and banks, while digital signatures prevent tampering. With the rise of quantum computing, the algorithms protecting these transactions could be broken, allowing attackers to decrypt sensitive banking information, forge signatures for fraudulent transactions, and steal funds from CBDC wallets.

3.2.3 Digital Certificates and Authentication

Digital certificates are used by websites to prove their identity to users through SSL/TLS protocols, relying on public key cryptography to verify the legitimacy of the site and prevent impersonation (R. Imam et al., 2021). Additionally, two-factor authentication (2 FA) systems use public key cryptography to secure methods like smart cards or security tokens. Quantum computers could break the cryptographic algorithms used in SSL/TLS certificates and 2 FA, leading to website impersonation, phishing attacks, and the compromise of authentication methods.

3.2.4 Software Integrity and Updates

Software integrity is maintained through code signing, where developers use digital signatures to sign software and firmware updates, ensuring that only trusted sources are providing the updates (PKI Consortium, 2013). Operating system updates also use public key cryptography to verify the authenticity and integrity of the update before installation. Attacks using stolen digital signatures to maliciously modify updates to system code, such as drivers, are well established (Page, 2022) (MITRE, 2018). Quantum computers could forge these digital signatures, allowing malicious actors to distribute compromised software disguised as legitimate updates without having to first steal and maintain legitimate digital certificates.

3.2.5 Digital Identity and Authentication

Digital identity systems, such as e-passports and smart ID cards, use public key cryptography to verify identities and authenticate users (Temoshok et al., 2024). Similarly, multi-factor authentication (MFA) systems employ public key cryptography to secure smart cards and

USB tokens used for secure logins. The rise of quantum computing could enable attackers to forge digital certificates, allowing them to impersonate legitimate users and gain unauthorized access to systems, leading to identity theft and security breaches.

3.2.6 Legal Documents and Contracts (e-Signatures)

Digital contracts are commonly signed using digital signatures, ensuring the signer's authentication and the document's integrity. Industries requiring regulatory compliance, such as finance and healthcare, depend on digital signatures for document validity. However, quantum computers could forge these digital signatures, rendering legal contracts vulnerable to tampering or fraud, and undermining compliance with industry regulations.

3.2.7 Encrypted Data Storage and File Transfer

Public key cryptography is used to encrypt files and data for storage and transfer, ensuring that only authorized users can access the content. This is commonly employed in cloud storage and secure file transfer protocols (e.g., SFTP). Quantum computers, with their ability to break encryption algorithms, could decrypt sensitive files, intercept data during transfer, and expose confidential information, posing a major security risk for both individuals and businesses.

3.2.8 IoT (Internet of Things) Devices and Smart Systems

IoT devices, including medical devices and smart home systems, use public key cryptography for secure communication and authentication. Firmware updates for IoT devices are signed with digital signatures to ensure that only legitimate updates are installed. Quantum computing could compromise these systems by forging digital certificates, allowing attackers to tamper with devices, intercept data, and install malicious firmware, jeopardizing the security of IoT ecosystems.

3.2.9 Healthcare and Medical Records

Protected Health Information (PHI), such as electronic health records (EHRs) and medical histories, are encrypted using public key cryptography to ensure patient privacy and prevent unauthorized access. Telemedicine applications also use cryptography to secure doctor-patient interactions and the transmission of sensitive medical data. Quantum attacks could enable attackers to decrypt EHRs, tamper with patient records, or interfere with secure telemedicine communications, endangering both privacy and healthcare security.

3.2.10 Government and Military Communications

Government and military organizations rely on public key cryptography to secure classified communications, ensuring that sensitive in-

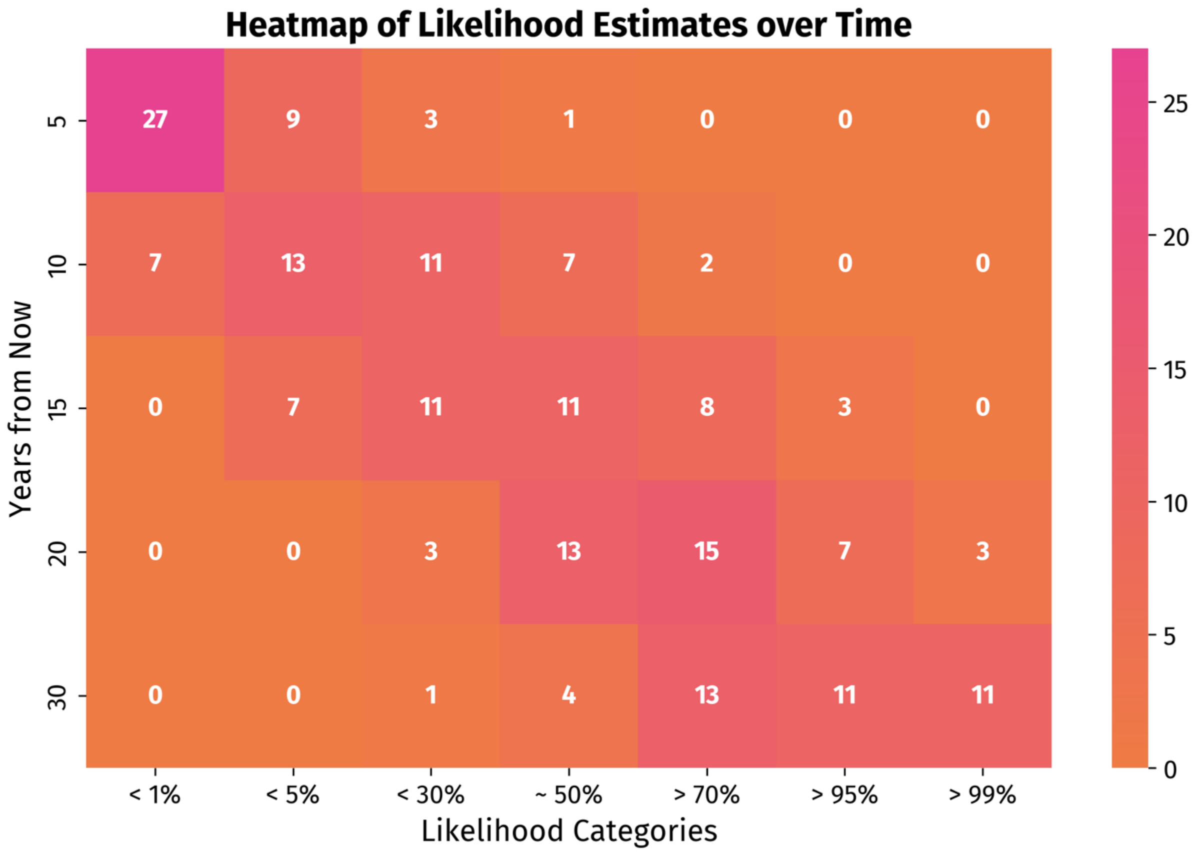

Figure 5 - Timeline Estimate of Quantum Threat Against RSA-2048 (Adapted from Mosca & Piani, 2022)

formation is protected from adversaries. Additionally, some online voting systems use cryptography to ensure the anonymity and integrity of votes. Quantum computers could break the encryption protecting these communications, leading to espionage or manipulation of voting results, potentially compromising national security.

3.2.11 Blockchain and Cryptocurrencies

Blockchain systems, such as Bitcoin and Ethereum, depend on public key cryptography to secure wallet addresses and authorize transactions. Digital signatures are used to ensure that only the rightful owner can initiate transactions, and consensus mechanisms like proof of stake rely on cryptography to validate blocks. If quantum computers can break the cryptographic algorithms underlying blockchain, attackers could steal funds, forge transactions, or manipulate consensus mechanisms. Additionally, quantum threats could lead to 51% attacks, where a quantum-powered adversary takes control of the majority of the network's computing power, allowing double-spending and ledger manipulation.

3.3 Race Against Time

The likelihood of a real quantum threat break-

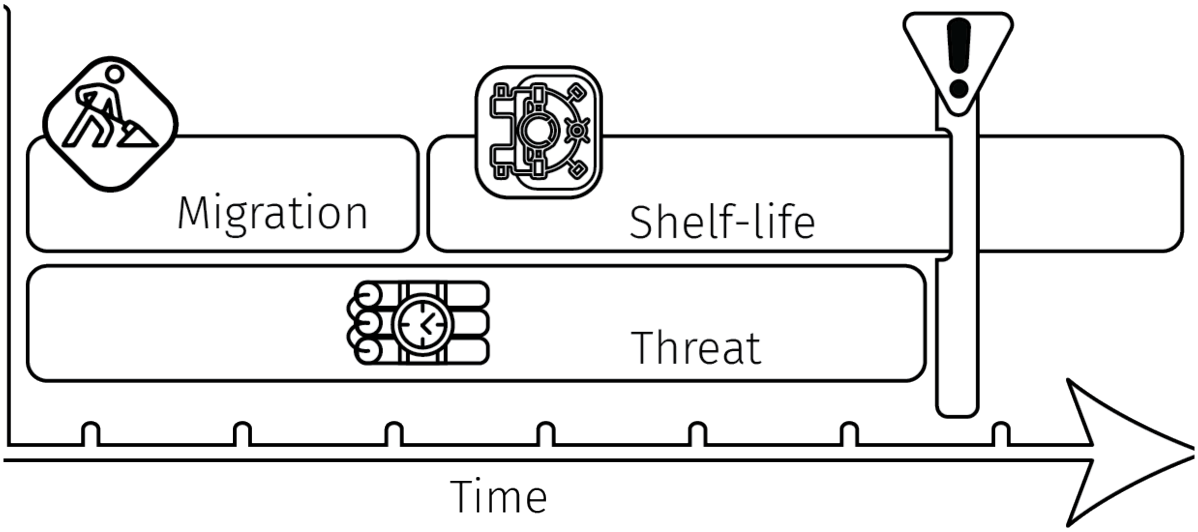

Figure 6 - Quantum Resistant timeline

ing public encryption is, in essence, a race against time. Some firms and governments are already preparing for a post-quantum world. This preparation is occurring despite current estimates that the emergence of a fully functioning quantum computer may be years away, with a survey of experts in 2022 suggesting that a functioning quantum computer with the ability to break RSA-2048 within 24 hours would be twenty to thirty years away (Mosca & Piani, 2022).

Nonetheless, the investment in mitigating the risks of such attacks could be argued to be prudent for several reasons. The possibility of harvest now, decrypt later attacks, the impact of the first uses of the technology and the legal repercussions of the technology.

3.4 Harvest Now Decrypt Later

A known cybersecurity risk from quantum computing is the opportunity for an attacker to conduct a “harvest now decrypt later” attack. Such an attack involves amassing large amounts of encrypted data to be stored until capacity for decryption becomes available (Fielder & Gunter, 2024).

Limited research has been devoted to investigating the consequences of this attack vector in quantum computing. This vulnerability poses serious risks, as it has been suggested that large corporations and adversarial states like China have been collecting large volumes of data, including state secrets, intellectual property and personal identifiable information (Sharma, 2021).

To mitigate against both broader encryption challenges and harvest now, decrypt later attacks, Mosca & Piani (2022) outline a risk framework as shown in Figure 6, which highlights the intersection between three areas of concern: the time it takes to migrate to quantum resistant infrastructure, the time that the data poses a potential for harm if exposed (i.e., the shelf life) of the harvested data, and the time until quantum computing technology poses a threat to the data.

Once the technology exists, there are other non-technical factors that may impact where its capabilities are deployed, meaning that the risk will not be shared equally across all sectors. Quantum computing is expected to be very expensive to power and run, and thus, a potential attacker faces an inherent opportunity cost. Accordingly, it can be expected that once functional quantum computers exist, they are likely to be used exclusively by the largest firms or most powerful governments, at least initially. As a result, the initial threat would be posed to the traditional targets of these well-resourced actors and then through the malicious utilization of the "quantum as a service" offerings. The costs and complexity of these attacks may see the initial threat being directed more towards military and governmental organizations or large organizations. As a result, we could expect that there would be some delay between the availability of quantum computing and the widespread decryption of internet traffic. It should be noted that, even in a post-quantum world, it may continue to be that case that simpler traditional cyberattack types such as using social engineering would be more cost-effective than quantum-based attacks.

3.5 Legal Implications

As noted previously, a major risk posed by the advent of quantum computing is the compromise of privacy in online encrypted communications and stored data. Since quantum computers would be able to break the traditional forms of encryption currently deployed by major messaging applications, the intimate communications between users could be subject to law enforcement surveillance (Kop et al., 2023). Similarly, encrypted data having a long shelf life held by organizations in the private and public sectors would become vulnerable (Bruno & Spano, 2021). In short, privacy rights in the era of quantum computing potentially face a two-pronged assault through data retention and access to encrypted communications.

3.5.1 Regulation of Data Protection

The Personal Information Protection and Electronic Documents Act (PIPEDA) is outdated; the Privacy Commissioner's office has limited resources, and it does not have the power to use strong enforcement measures to ensure compliance (Office of the Privacy Commissioner of Canada, 2022). The Office of the Privacy Commissioner works through a mix of recommendations and minimal fines (Personal Information Protection and Electronic Documents Act, 2000), which are not sufficient to ensure accountability for the private sector organizations. Regulating data retention in the public sector is especially complicated because different organizational needs mean some institutions have legitimate needs for retaining personal information for longer periods as opposed to the private sector, wherein retaining data is tied to commercial interests.

Bill C-27, which is currently being considered in the House of Commons, proposes some changes in the right direction, as it allows imposition of penalties proportional to the revenue of organizations but caps them at $10,000,000

(Bill C-27 - An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, 2022).

Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, was recently passed by the House of Commons and is in its second reading stage at the Senate (Bill C-26 - An Act Respecting Cyber Security, amending the Telecommunications Act and making consequential amendments to other Acts, 2022). The bill introduces cybersecurity obligations for four federally regulated critical cyber systems, like financial services, energy, telecommunications and transportation. The Critical Cyber Systems Protection Act (CCSPA) would introduce obligations to ensure good cybersecurity practices amongst the regulated sectors, which include reporting cybersecurity incidents to the Communications Security Establishment (CSE), supply chain obligations and enforcement of cybersecurity directions through administrative monetary penalties. While a step in the right direction, the bill falls short of addressing the quantum threat, as it is agnostic to technology and does not create much emphasis on cryptographic agility (Bill C-26 - An Act Respecting Cyber Security, amending the Telecommunications Act and making consequential amendments to other Acts, 2022).

3.5.2 Data Retention by Private and Public Sector

Many private organizations tend to retain data for longer than would be reasonably understood as necessary. For example, in the investigation into the data retention practices of *Ashley Madison*, Avid Life Media was found to have retained data of users who had deleted their accounts, remained inactive for extended periods of time and even paid ALM to “fully delete” their profiles (Office of the Privacy Commissioner of Canada, 2016). Such practices present unnecessary risks to current and former clients of these operators should this data become vulnerable by means of quantum computing threats in the future. Some information retained by organizations has a long-shelf life, in that the possibility of harm is long lasting. This data might include evergreen contact information and biometrics. This threat is not limited to industry, as public sector organizations also hold personal information for extended periods of time, which poses similar risks.

It is clear that there is an urgent need to reform Canada’s privacy legislation. Keeping in mind the disproportionate risk to long-term information caused by quantum computing, stringent regulations are required to enforce data minimization and ensuing that there is no retention of data beyond the period necessary will likely require effective enforcement of penalties. This would help data holders to mitigate the risks of bad actors harvesting data to be used later. The principles of privacy by design provide a mechanism for organizations to manage these requirements.

Strict deadlines should be imposed for reporting data breaches to the Privacy Commissioner along the lines of the 30-day deadline approach taken by the Federal Communications Commission in the USA (Federal Communications Commission, 2023). Companies should work in conjunction with other entities in their supply chains to ensure that cybersecurity practices followed by all of them are harmonized.

To ensure that any reforms to Canada's privacy legislation have teeth, the Privacy Commissioner's office must be resourced and empowered with the ability to enforce their recommendations/decisions. Bill C-27 has taken steps in this regard; however, due to the capping of penalty limits, its deterrent effect will be limited.

3.6 Regulation of Quantum Computing

In its current form, PIPEDA imposes the requirement of having security safeguards in line with the sensitivity of information. This provision may become outdated with the advent of quantum computing. Considering the importance of preserving data and interests of small businesses, the new security safeguard regulations should take a tiered approach. These regulations should be implemented through industry standards supported by soft law instruments.

Large platforms and small platforms holding sensitive long-term data should both conform to the highest standards of protection, reflecting their significant societal impact or the critical nature of the data they manage. In contrast, remaining small platforms, which handle less sensitive information, should focus on future-proofing by preparing a transition plan to adopt post-quantum cryptography within a timeframe set by regulations. This approach ensures robust security for critical platforms while promoting practical, scalable measures for smaller entities.

Large Platforms	These platforms should be required to conform to the highest standards of protection.
Small Platforms Holding Sensitive Long-term data	These platforms should be required to conform to the highest standards of protection.
Small Platforms	These platforms should prepare a transition plan of shifting to post-quantum cryptography within a stipulated number of years (to be determined by regulations).

A tiered approach would ensure that small businesses are not left at a competitive disadvantage due to the costs of shifting to post-quantum algorithms. Large organizations are considered to be digital platforms that, in line with the description set out in Bill C-18, earn a total global revenue of CAN$1 billion or more in a calendar year; and have 20 million or more Canadian average monthly unique visitors or Canadian average monthly active users. These platforms are considered to be of sufficient reach that their security impacts Canadian society and possess sufficient resources to comply with the measures.

Following best practices common to cybersecurity in general, both large platforms and small platforms that deal in sensitive information should designate a person to prepare regular reports on the post-quantum resistance measures deployed by the platform and residual small platforms should designate a person to prepare regular reports documenting measures taken in transitioning to post-quantum algorithms.

3.6.1 National Security

From a national security perspective, quantum computing technologies having data security risks could be regarded as dual-use technologies and consequently be subject to export controls once the technology becomes a reality. If the technology is developed at such a time as to present a danger to Canadians, Canada could canvas for its inclusion in the export control list under the Wassenaar Arrangement (Dekker & Martin-Bariteau, 2022). Canada's National Quantum Strategy emphasizes international collaboration in the development of quantum technologies. However, a measured approach should be taken in the case of quantum applications causing risks to information security with primacy should be given to protecting data of citizens rather than collaborating with other states (Government of Canada, NQS).

3.6.2 Law Enforcement

From a constitutional perspective, a question arises about the merits of allowing law enforcement access to encrypted data through quantum computing technologies. Such a system, if deployed by the state in case of private communications, runs a risk of conflicting with the right against unreasonable search and seizure guaranteed by Article 8 of the Canadian Charter of Rights and Freedoms (1982).

Provisions to allow law enforcement access to private encrypted communications through quantum computing could go a long way in enhancing the investigative techniques but could also open doors for the misuse of those same technologies against Canadian citizens by adversarial foreign actors, as has happened with similar provisions in the United States (Cybersecurity & Infrastructure Security Agency [CISA], 2024). Given Canada's constitutional framework surrounding minimal intrusion for searches (*Goodwin v British Columbia*, 2015), judicial authorization could possibly be refused by courts. Meanwhile, the adversarial actors would be able to benefit by using the same technology against Canadian citizens. As a result, the impact of instituting such a system would have to be carefully weighed against the risks it could pose.

There is a reasonable expectation of privacy associated with regular private messages (*R v Marakah*, 2017). The existence and use of encryption lends more strength to the subjective expectation of privacy. Following the turn of the century, a normative surveillance-based approach towards assessing privacy risks has become mainstream as opposed to a traditional risk-based approach (Stewart, 2011, *R v Bykovets* 2024). A surveillance-based approach towards privacy sets a high bar for the use of investigative techniques, as they should be performed in a manner that would not raise concerns regarding violation of rights guaranteed by the Constitution (Stewart, 2011). Considering the possibility of access to communications with such a powerful tool as quantum computing decryption, it would be necessary to reassess the methods of law enforcement access to private messages. The careless use of quantum technologies by law enforcement should be discouraged to avoid their use being ruled

3.6.3 Minimizing the Differential impact of Quantum Technologies.

Like any new technology, quantum technology is not inherently positive or negative. The impacts are ultimately determined by the people who create and implement it (Wolbring, 2022). Past experiences with new technologies have indicated that their impact can vary greatly throughout society. Advances such as the printing press, railways and facial recognition have not impacted all members of society equally (Bill of Rights Institute, n.d.; Bongiorno, 2020; de Boer, 2023; Fussell, 2020). It is therefore important to understand the potential for harm and make efforts to reduce the negative impacts of any new technology.

Digital inclusion centred on intersectionality is essential for including the already vulnerable and marginalized groups that face the highest risk of social and economic exclusion in a post-quantum world (Tsatsou, 2022). An intersectional approach will allow researchers, policy-makers, funders, and government stakeholders engaged in preparation for quantum technology to be cognizant of the multidimensionality of diverse identities and lived experiences of users who will be the most affected (Crenshaw, 1991; Tsatsou, 2022). This will also help further address current digital divides, barriers and vulnerabilities that already exist and have a high potential to be reproduced in a post-quantum world (Roberson, 2022; Tsatsou, 2022). While it is not the only framework to take into consideration, an intersectional approach will help emphasize *diverse and complex* aspects of a user's *social* identity, and how their unique social identity may interact with quantum technologies to create barriers or inequities in digital spaces (Crenshaw, 1991; Bešić, 2020). Furthermore, a quantum education pipeline designed to ensure the developing capabilities of digital technologies is understood will be critical in shaping and inspiring the next generation of Canadian quantum experts and workforce to think about the possible futures of a post-quantum world (Wolbring, 2022; Siberman, 2022). This will also address potential skill gaps in relation to quantum technologies in the future workforce, positioning Canada to be a quantum leader globally.

3.6.4 Education on Quantum Technologies

Amplifying education and awareness of quantum technology will be critical for all users, as they are also ultimately the consumers of quantum-related technological advancements. Increasing consumer knowledge on the effectiveness of current quantum-proof algorithms is important for underpinning an effective market for post-quantum encryption. The more educated users will be on policies, regulations, and the current discourse on quantum technology, the more they will want to engage in processes of succession and planning for a post-quantum world (Graz & Hauert, 2019). Education efforts targeting consumers of quantum-related technologies will aid in managing consumer expectations of what they are purchasing from companies and how secure post-quantum encryption is.

Education and awareness of the "store now, decrypt later" threat for all users can highlight the need for increased vigilance about current cyber behaviours and the types of data shared online – personal and sensitive information posted now can be vulnerable to post-quantum encryption in the future. Users do not have to wait for a quantum computer to arrive to practise good cyber security practices that protect their data online. While the advent of quantum technology will bring about a new set of norms and standards in digital spaces, current research has found that most users do not practise adequate cyber hygiene (Argyridou et al., 2023; Cain et al., 2018). This means that all levels of Canadian government must continue to collaborate and organize basic cyber education and awareness for the public. It is important to highlight tools that safe digital behaviours so that users of all ages and backgrounds can uphold personal security and maintain a line of defence against cyberattacks – near or in the future (Neigel et. al., 2020).

4 Known-Unknowns

Researchers and manufacturers have started to develop small-scale quantum computers (Gambetta, 2023). However, to the best of our knowledge, a publicly available quantum computer that can solve classically hard problems does not yet exist (Gambetta, 2023; Mosca and Piani, 2022). Multiple factors, such as noise/decoherence, error correction, and controlled environment, affect the efficiency and accuracy of quantum computing (Gidney and Ekerå, 2021; Mosca and Piani, 2022). Therefore, there is no consensus amongst researchers on the exact year when quantum computers will be able to factorize an RSA 2048-bit integer within 24 hours (Mosca and Piani, 2022). However, experts predict that it is likely that we may be able to create such quantum computers within 30 years (Mosca and Piani, 2022). Due to the current limitation of building a quantum computer with revolutionary computing capability, researchers are unable to experiment, verify or conclude their educated guesses. Researchers generally agree that quantum computers can evaluate certain problems at a much faster rate than classical computers and that there is an implication on cybersecurity (CCA, 2023). The limitation of the current state of quantum computing technology also affects the development of effective risk assessment and mitigation strategies, since many proposed uses of quantum computing are currently largely hypothetical. The next section will discuss the foreseeable hypothetical quantum computing threats, applications and risk assessment strategies that we can identify and of which we will attain more understanding in time but are at current limited to certain conclusions due to the present quantum computing limitations.

4.1 Authentication Systems

In a post-quantum era, the current, or classical authentication systems that rely on encryption in order to maintain confidentiality may be rendered obsolete. These systems rely on cryptography in order to exchange secrets (e.g., passwords) in public and to store such secrets securely. This would affect all publicly accessible web applications with authentication mechanisms and impact everything from how authentication secretes are inputted, verified and stored (Szikora and Lazányi, 2022).

While numerous techniques have been suggested as to how we can approach securing password authentication from quantum computers, further research efforts are required to confirm such findings. Some examples of the explored techniques of making authentication systems resistant against quantum computers include quantum resistant two factor/multi-factor authentication schemes (Wang et al., 2021), quantum safe key agreement protocols (Li et al., 2022) and a quantum resistant single sign on scheme (Jiang et al., 2022). While these methods offer promise, they aren't without criticism (Qin et al., 2022). Furthermore, as capable quantum computers are not available to researchers, it is not possible to know precisely how these schemes and their implementation will perform against quantum aided decryption techniques. Regardless of how well they perform in theory, our experience with mechanically and classically computed encryption schemes has shown that there are many problems to solve beyond the mathematics. As such, it is important to emphasize that additional research and validation are necessary to verify the techniques.

As a mitigation strategy, companies can at the minimum begin to secure their secrets (i.e., customers' passwords, messages or stored data) with the post-quantum cryptography standards suggested by NIST soon (NIST, 2024). Doing so will provide at least the prospect of security. Further, they may also consider how they can make their authentication systems more modular or "agile" such that future changes in authentication or the cryptographic algorithms itself can be implemented quickly and independently (cyber eco, 2024).

4.2 Cyber-Physical Systems (CPS)

Cyber-Physical Systems are systems that integrate computation into physical processes where the software and physical components are often intertwined to enable benefits such as safety, scalability, and capability (NSF, 2024). CPSs perform automated controls in the physical equipment found in a range of systems, from medical monitoring devices and smart grids to large-scale SCADA (Supervisory Control and Data Acquisition) systems (Colbert, 2017). It is prevalent in Critical Infrastructure, including transportation networks, nuclear power plants, electric power grids, water and gas distribution systems and more (Colbert, 2017). Cybersecurity is a growing concern for CPSs, especially in our Critical Infrastructure systems, as more insecure IoT devices or remote network installation are incorporated in their previously isolated network infrastructure (Colbert, 2017).

Quantum capabilities pose a threat to such critical infrastructure, as many of the techniques required to make communications in CPSs systems secure are reliant on classical cryptography (Tosh et al., 2020). Due to the emerging quantum computing technology, there is a concern that critical communication in such systems may no longer be confidential as intended, especially with the rising deployment of IoT devices in such critical infrastructures (NIST, 2023). The Canadian government has made it clear that this is an area of concern in the upcoming future (QRWG, 2023).

The nature of these systems presents a particular issue with regards to quantum technologies. The critical nature of these systems makes reliability a primary concern, as their operation often affects the safety of individuals and communities. Resultingly, updating these systems requires a greater period of testing to ensure changes to not adversely affect primary functions under any circumstances and dynamic capability adjustment through over the wire patches are less likely or desirable. Systems are often optimized more tightly for their particular purpose and resultingly do not have available processing overhead for more complex cryptographic schemes, meaning that systems may have to be replaced or augmented in order to provide post-quantum safe operation. As a result, the updating of these systems to make them quantum resistant may require a greater amount of time and require clear guidelines to ensure durable implementations.

As the technology for quantum computing is not mature yet, it has not been straightforward to provide definitive guidelines, policies or mandates to make critical systems secure against quantum (QRWG, 2023). Governing bodies can only highlight the significance of being aware of the threat and suggest a high-level recommendation of how the nation can begin to address the problem for now for the upcoming future threat (QRWG, 2023). Canada has urged Critical Infrastructure (CI) owners to begin considering the adoption of quantum safe cryptography into their current systems. A national guideline of the migration towards quantum safe CI systems has been published to recommend the best practices for Canadian CI operators and other stakeholders (QRWG, 2023). The guideline highlights that while it may appear like quantum computing is a distant threat towards CI systems today, the best way to prepare for it is to start proactively addressing the threat now, as the repercussions of quantum threat distributing CI systems are significant at a large scale and the migration to post-quantum cryptography could also take time (QRWG, 2023). It will require efforts from organizations at a national scale, both in the public and private sector, to collaboratively ensure quantum resistant systems in our CIs. As a broad minimum, engineers should begin to think about how classical encryption can be replaced by post-quantum cryptography algorithms, for example securing the secrets between sensors and processor components (Tosh et al., 2020).

4.3 Accessibility to Quantum Computers

The capability for nations to manufacture leading technology is dependent on many factors, including economic, resources (physical or intellectual) and political considerations (CCA, 2023). There is a global race to develop a fault-tolerant quantum computer and is explicitly addressed as a strategic advantage by many countries (Mosca and Piani, 2022). Sources suggest that, as far as we know, North America is leading in the race (Mosca and Piani, 2022). However, it has been transparently stated that this is only based on publicly provided information and responses provided by other countries about their progress in quantum technology advancement (Mosca and Piani, 2022). It is difficult to determine the extent of other advancements from other countries (or even other organizations within those countries) that have the motivation to maintain confidentiality on quantum computing capability (Mosca and Piani, 2022).

The varying availability of quantum computers between countries creates concern about the potential impact of unequal quantum capabilities between nations (CCA, 2023). It is difficult to predict whether forefront countries will be willing to manufacture quantum capable computers to other countries (CCA, 2023). It is also difficult to predict what the repercussions would be if a country is behind in quantum development and how they can expedite their advancement after quantum computers become readily available. We can only present an assumption that they will be vulnerable to many exploits that they are unprepared for.

One possible option is to try to create a level playing field between allies and push the technological forefront together by collaborating internationally in both the public and private sector while maintaining an exception to this interchange for adversarial nations (Mosca and Piani, 2022). It is hypothesized that as geopolitical tensions shift, there may be an increase in the amount of spending towards developing quantum computers, which could drive a separation between countries based on their available resources. Without sharing, this could be disadvantageous in the long term, as the deterioration of trust may create challenges for international collaboration, resulting in a reduction in the advancement of quantum computing technologies. Based on this possibility, it may be in the best interest of all countries to maintain collaborative alliances to provide for the greatest likelihood of scientific progress (Mosca and Piani, 2022).

At a more granular level, there is a similar concern for the disparity in access to quantum computing between organizations (CCA, 2023). Unequal access to quantum computing may result in the concentration of quantum development within only a handful of companies. This may lead to biases being unintentionally developed into quantum solutions, which may disaffect minorities or smaller socio-economic groups, as has been observed in AI decision making applications (CCA, 2023). Providing access to a range of organizations, including smaller and medium-sized enterprises, may allow for development to reach further across society so that potential issues of this type may be identified and corrected early.

How to enforce safe practices for cooperation remains an unknown challenge, as powerful, fault-tolerant quantum computing technology is still not widely used in businesses (CCA, 2023; Mosca and Piani, 2022). However, efforts have been initiated to address the potential digital divide between small and large corporations by drawing lessons from historical policy impacts and societal responses to technological advancements that have had systematic effects (CCA, 2023). Proposed strategies for adopting quantum technology responsibly include controlled access to quantum systems, the development of soft law frameworks, and the promotion of responsible research and innovation (CCA, 2023). Overall, industry appears to recognize that disparities in quantum capabilities can create significant disadvantages, which has prompted investigations into safe quantum adoption practices (CCA, 2023; Mosca and Piani, 2022).

4.4 Quantum computing – a reset for current risk assessment practices?

Predictions about the societal impact of quantum computing range from as revolutionary as the discovery of fire (Francis, 2022), to a "a self-denying prophecy" pre-emptively mitigated by countermeasures, particularly in cryptography (Lindsay, 2020). The variance in these estimates reveals the difficulties quantum computing presents for those assessing its risks. Identifying the risks, their distribution, and their impact across individuals, organizations, and governments is essential for developing effective cybersecurity strategies. Quantum computing's wide-ranging applications in finance, pharmacology, defence, and beyond create risks that are diverse and unevenly distributed, challenging existing risk assessment frameworks (Porter, 1990; Witt, 2022).

The presence of national and international demand conditions, resource endowments, and significant capital investments in quantum computing further complicate accurate predictions about threats. The cross-domain nature of quantum computing applications means that conventional methodologies like ISO-31000 struggle to adequately address its risks. This section critiques traditional frameworks, explores their limitations, and introduces models from medicine, biopharmaceuticals, and climate science as potential inspiration for methods to better evaluate quantum-related risks.

4.4.1 Traditional risk management frameworks (ISO-31000)

ISO-31000, introduced in 2009, underpins risk management worldwide. Its structured process assesses risks sequentially: identifying exposures, evaluating severity and likelihood, implementing controls, and monitoring residual risks (Dali & Lajtha, 2012; Lalonde & Boiral, 2012). The model's strengths in its scalability, transparency, and applicability across disciplines as resulted in it being widely adopted as a "gold standard". In Canada, for example, the Government of British Columbia (2022), the Treasury Board Secretariat (2016), and Public Safety Canada (2024) all explicitly reference ISO-31000 for use in risk assessment and risk management practices. Further, the Harmonized Threat and Risk Assessment Methodology for cybersecurity (Communications Security Establishment, 2007) shares a similar methodological orientation.

Problematically for Quantum Computing applications, this approach often compartmentalizes risks, treating them as discrete, domain-specific issues. For instance, the UK's National Risk Register evaluates 89 threats individually (HM Government, 2023), neglecting the interactions between risks, particularly those spanning multiple domains. While this enables structured evaluations, the model's emphasis on compartmentalization overlooks the dynamic interplay of risks that may arise in a post-quantum world. Identifying risks in isolation simplifies management but misses cascading and interconnected threats that require a holistic approach.

4.4.2 Domain Specificity and Heuristics in Risk Assessment

Risk assessment is inherently human-centric, shaped by perception, cognition, and judgment. This reliance introduces biases and oversights, particularly when addressing risks with transdisciplinary implications, such as cyber threats (Papamichael et al., 2024). Current practices often fail to anticipate cascading risks stemming from globalization and interconnected systems, as demonstrated during the COVID-19 pandemic (Sachs, 2022).

The risk-by-risk evaluation model promoted by ISO-31000 emphasizes domain-specific assessments, often stumbling against the diverse environmental (e.g., legal, governmental) contexts of modern risks. Assessing risk horizontally is hampered by the human limitations in perception, cognition and judgment due to the complexities of such environments. Heuristics further complicate accurate risk evaluation. Assessments can by biased by external factors such as the emotional state of the assessor as well as other more directed biases such as conformity, framing and availability biases. Recognition of such biases is critical to enhancing existing frameworks. A shift towards understanding risks as interconnected phenomena is essential for addressing quantum computing's transnational and cross-domain challenges. As a result, a systematic approach that incorporates cross domain and anti-silo approaches while reducing the negative impact of heuristic decision-making would be beneficial for such complex systems of risk.

4.4.3 Risk Assessments in Complex Systems of Interactions

The study of interactions can be found in medicine, biopharmaceutical manufacturing and climate science that acknowledge the dynamic interrelationship between risks and the unknown. There are frameworks from medicine, biopharmaceuticals, and climate science demonstrate methodologies that offer insights for working with quantum computing risk.

Medicine: The Sequential Organ Failure Assessment (SOFA) score is widely used in intensive care units to monitor organ system interactions. By evaluating the functioning of six organ systems at admission and at regular intervals (Lambden et al., 2019), the SOFA score incorporates the potential for medical incidents in one system to cascade into others, influencing patient outcomes. This approach highlights the importance of viewing risks as dynamically interlinked rather than as static, isolated events.

Biopharmaceuticals: In biopharmaceutical manufacturing, interaction matrices are employed to assess how changes in one operational parameter impacts others (Meitz et al., 2014). These matrices identify interdependencies within production processes, enabling adjustments that minimize negative cascading effects. This framework is particularly relevant to quantum computing, where advancements in hardware or algorithms may trigger far-reaching consequences across interconnected systems.

Climate Science: Climate risk models address the complexities of overlapping hazards. Simpson et al. (2021) developed a framework to ex-

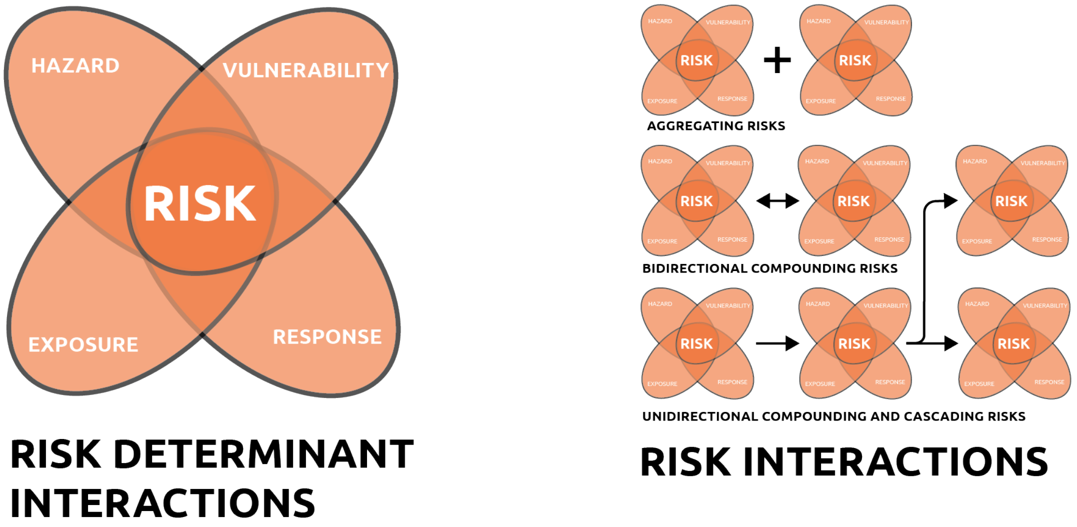
HAZARD
VULNERABILITY
RISK
EXPOSURE
RESPONSE
RISK DETERMINANT INTERACTIONS
AGGREGATING RISKS
BIDIRECTIONAL COMPOUNDING RISKS
UNIDIRECTIONAL COMPOUNDING AND CASCADING RISKS
RISK INTERACTIONS

Figure 7 - Interactions between determinants, and interactions of drivers within and between determinants of risk (adapted from Simpson et al., 2021)

amine interactions between climate risk determinants, such as bidirectional feedback loops, unidirectional influences, and aggregate impacts. For instance, their model analyzes how localized environmental changes can escalate into broader systemic threats. The figure below illustrates this framework, emphasizing the importance of capturing relationships between risk drivers to predict and mitigate cascading effects effectively.

These frameworks underscore the necessity of adopting integrated approaches for risk evaluation. By leveraging insights from these diverse fields, organizations can better navigate the multifaceted risks posed by quantum computing, improving both predictive accuracy and the robustness of response strategies.

4.4.4 Towards a Model of Interaction and Integration

Addressing cybersecurity risks in a post-quantum world requires moving beyond ISO-31000's domain-specific frameworks. While it may be a difficult task to overcome the inertia of the status quo, the rapid pace of technological innovation necessitates new risk management frameworks that account for transnational threats and the limitations of human judgment.

We argue for a systems-based approach that integrates traditional risk management practices with models emphasizing interdependencies. Such frameworks could enable organizations to better navigate the complexities of quantum computing's cybersecurity impact, fostering resilience in a dynamic, interconnected world. Acknowledging the interplay between human biases, organizational inertia, and rapidly evolving technological landscapes is crucial to building robust frameworks for future challenges.

5 Unknown-Unknowns

5.1 Critical raw materials, components and equipment

The design and deployment of quantum computers rely on the availability of particular physical materials from the natural world. These resources are finite and unevenly distributed geographically, which could lead to competition between nations and industries. However, the availability of these materials may change over time and demand for specific minerals depends on an evolving set of technologies. As a result, the impact of the availability of these materials is unknown.

The Stanford Center for Responsible Quantum Technology is examining the links between critical raw materials—such as tantalum, tungsten, lithium, and cobalt—the availability of components and equipment, and supply chain vulnerabilities (Lee, 2023). China and Southeast Asia are major exporters of these minerals, and their supply chains are vulnerable to disruptions from export restrictions, natural disasters, and regional or international conflict.

As Lee (2023) notes, the utility of raw materials depends on their role in components and the specialized equipment combining these components for various functions. Both materials and equipment are susceptible to supply chain disruptions and cross-border dependencies. Accordingly, an understanding of the raw materials, components and equipment necessary and the interplay between these elements for quantum computing development and deployment is critical to Canada's long-term defensive and strategic interests.

The Government of Canada is uniquely positioned to coordinate, guide and disseminate the evaluation of the complex interdependencies in quantum computing-related supply chains by leveraging the knowledge of industrial and academic institutions and those of its allies. For example, Canada's Critical Minerals Strategy (2023) could be further developed to the evaluate materials required for quantum computing technologies, and harmonized with Canada's National Quantum Strategy (2023). Components and equipment, including innovations in material sciences on new compounds with quantum application (Serrano et al., 2022), should also be incorporated into broader supply chain risk assessment of geographical interdependencies.

Canada's endowment of natural resources within its geographical borders and related industries offers the country a highly competitive strategic position for the quantum era. Protecting these advantages, and leveraging them in corporation with allies, will be central to Canada's long-term national security interests in an increasingly uncertain and hostile geopolitical environment.

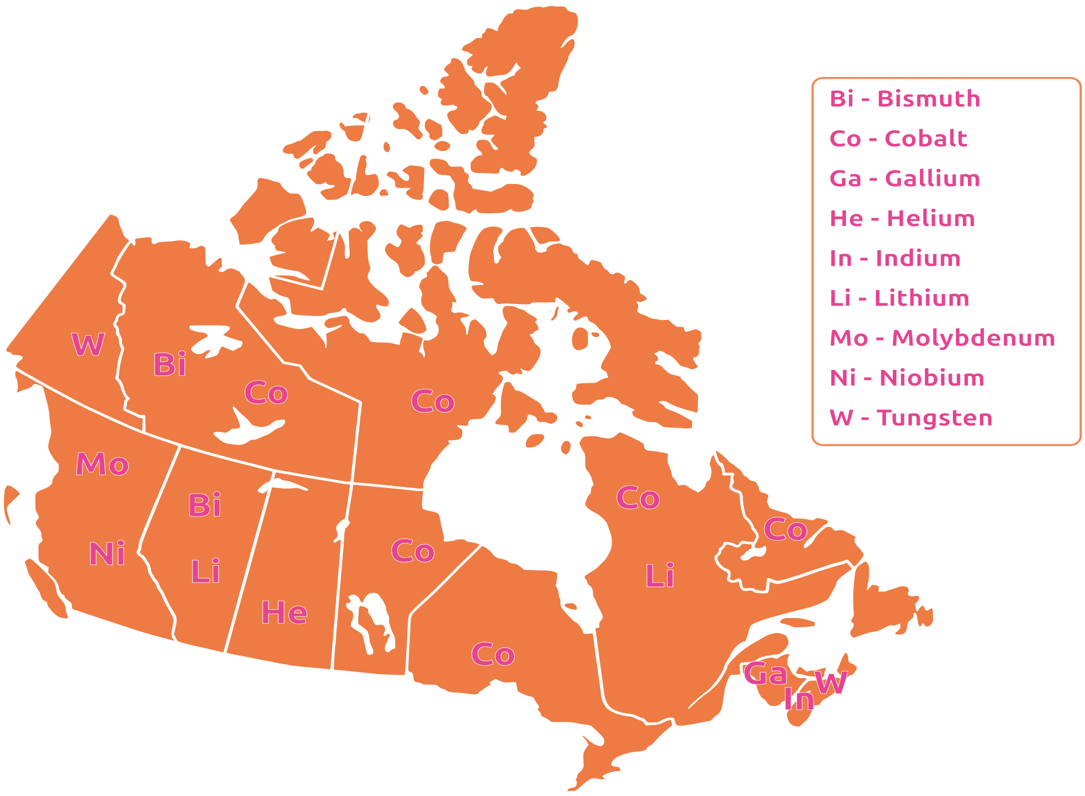

Figure 8 - Canada's Critical-Mineral-Rich Regions, highlighted with select minerals with quantum applications (Government of Canada, 2022, Lee, 2023)

5.2 Blockchain and Cryptocurrencies

The impact of quantum computing enabled attacks on blockchain-based technologies is not well understood. Currently, blockchain technology, often praised for its decentralized nature, and enhanced security over traditional digital ledgers, has been rapidly developed for use in many applications. Current and future applications of Blockchain technologies include Non-Fungible Tokens (NFTs), Decentralized Autonomous Organizations (DAOs), Cross-Border Payments, Intellectual Property and Digital Rights, Anti-Counterfeiting and Provenance, Supply Chain Management, Internet of Things (IoT), Healthcare Data Management, Smart Grids and Energy Management, Voting Systems and Identity Management. While most of the current implementations of these technologies do not make use of quantum-resistant cryptography, the wide range of domains and rapid development make it difficult to determine associated risks.

Importantly, blockchain is also the foundation for many cryptocurrencies. However, blockchain technology remains vulnerable to a quantum attack (Gao et al., 2018). While several quantum resistant schemes have been proposed, there are, as of yet, no operational quantum resistant cryptocurrencies. Nonetheless there are promising foundational efforts, such as the “Quantum Resistant Ledger”, a blockchain protocol specifically designed to be resistant to a quantum attack (QRL, 2024).

While there are many aspects to these different technologies where they are being used for critical infrastructure, such as the potential for government-backed central bank digital currencies (CBDC’s), it is important to understand how little is known about both the extent and impact of quantum computing on blockchain and related technologies, particularly cryptocurrencies.

5.3 Quantum Computing and AI

The impact of the combination of Artificial Intelligence (AI) technologies and quantum computing is difficult to anticipate. There are possible use cases for combining quantum computing with AI. Most researchers look at the combination of the two technologies, like using AI to help with quantum computing cases or quantum computing to help with AI cases (Ying, 2009).

A key bottleneck for large-scale models (such as LLMs with hundreds of billions of parameters) is the enormous training time. Quantum computation could speed up the training processes used to develop AI technologies, potentially cutting down days or weeks of training to much shorter times. Quantum technologies, therefore, could have an impact on the capabilities provided by Artificial Intelligence. However, the extent of the benefits or feasibility due to the resources required are as yet unknown.

Artificial Intelligence could be combined with Quantum computing to enhance the targeting of decryption efforts through automated vulnerability discovery. This combination could also include the use of AI tools to aid with the interpretation and analysis of decrypted large-scale datasets.

Some possible quantum AI use cases are quantum algorithms for learning and for decision problems, quantum searches, and quantum game theory (N. Jyothi Ahuja and S. Dutt, 2022). These approaches could provide support for nations using them for strategy simulation and weapons systems optimization.

The impact of the combination of these technologies is unknown. AI technologies are rapidly developing and their capabilities at the time that reliable quantum computing technologies are available are difficult to predict. Furthermore, each of these technologies are demanding in terms of energy resources.

6 Recommendations

1. Continue to incentivize standardization of post-quantum encryption infrastructure for major targets:

   o **Provide support for the more vulnerable businesses and groups (SMEs). This may be achieved through financial incentives such as tax breaks for using quantum resistant technology such as certain service providers. Another possible solution is through government programs similar to the Home Accessibility Tax Credit.**

2. Conduct and fund independent research on the implications of quantum tech-

nology:

- o Harvest now, decrypt later issue
- o Impact on different stakeholders, SMEs, marginalized groups
- o This could be achieved via prioritizing federal academic funding through agencies such as NSERC and SSHRC

3. Consider a mix of hard legislation and soft law instruments to mitigate threats from quantum computing:

- o Data protection requirements should be enforced through concrete legislations
- o Security standards can be embedded through soft law instruments like guidelines or codes of conduct.
- o Guidelines for the use of quantum decryption tools by law enforcement to ensure use does not violate constitutional laws
- o Potential export control for weaponized applications of quantum technologies.

4. Effective information/education campaigns for individuals of different backgrounds (i.e., primary, secondary, college/university, older adults, marginalized communities) (Carley, 2020)

5. Re-evaluate threat and risk assessment frameworks to incorporate the assessment of interaction *between* risks and interdependencies across space and time.

6. The Government of Canada can take a leadership and coordination role to assess interdependencies in supply chain risks relating to critical materials, components and equipment for quantum computing development.

7. Continue to seek collaboration with international partners to ensure the responsible development of quantum technologies globally.

7 Conclusion

This report has examined formal academic research in addition to numerous other resources to learn more about quantum computing and what this means for cybersecurity. In particular this research has investigated how quantum computing will disrupt cybersecurity, how cybersecurity threats should be mitigated and how Canada in particular should prepare for a quantum future across multiple disciplines.

By taking the approach of identifying problem areas in terms of a known-knowns, known-unknowns, and unknown-unknowns framework, the report provides a novel perspective on quantum computing and cybersecurity.

We have presented how quantum computing will disrupt cybersecurity has been addressed by illustrating the imminent threat to confidentiality by means of encryption, a clear known-known scenario. In terms of known-unknowns, while we can anticipate attacks such as harvest now, decrypt later, the precise timing and scope of their execution remain uncertain, highlighting the need for ongoing research and proactive policy measures. The final category, unknown-unknowns, includes emerging concepts such as the intersection of quantum computing with AI and blockchain, where the full extent of risks and their ramifications for society and regulation are yet to be fully understood.

These distinctions directly inform our recommendations. Immediate action is required to standardize post-quantum encryption and strengthen data protection regulations, directly addressing the known-known vulnerabilities. Strategic investments in interdisciplinary research and adaptive risk management frameworks can clarify known-unknowns, ensuring that stakeholders remain agile as quantum capabilities evolve. Forward-looking policies, inclusive educational efforts, and ongoing international cooperation aim to reduce the likelihood of unknown-unknown threats catching us unprepared. By clearly aligning each recommendation with the challenges identified, we offer a roadmap that does not just reiterate the issues, but guides stakeholders in taking timely and effective action.

On top of this, the report also speculates on some less concrete but likely relevant areas of cybersecurity to be impacted by quantum computing such as quantum AI and quantum blockchain. Lastly, this research has compiled a list of proactive recommendations that, if successfully implemented, should allow us to win in the race against time with respect to the emergence of the quantum threat and avoid repeating the mistakes of the past.

It is hoped that decision-makers, technologists, and the public can use this understanding to prioritize resources, refine policies, and cultivate resilient digital ecosystems. The ultimate goal is to maintain trust, protect privacy, and ensure that quantum computing's transformative potential can be harnessed securely, equitably, and responsibly.

8 References

Abdikhakimov, I.. (2024). The interplay of quantum computing, blockchain systems, and privacy laws: challenges and opportunities. https://elita.uz/index.php/jurnal/article/view/37

Abraham, M., Crawford, J., Carter, D., & Mazotta, F.. (2000). Management decisions for effective ISO 9000 accreditation. https://www.emerald.com/insight/content/doi/10.1108/EUM0000000005346/full/html

Adams, M., & Makramalla, M.. (2015). Cybersecurity skills training: an attacker-centric gamified approach.

Apple. (2024). Imessage with pq3: the new state of the art in quantum-secure messaging at scale. https://security.apple.com/blog/imessage-pq3/

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S.. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: concept study. *Journal of Medical Internet Research*, . https://www.jmir.org/2023/1/e41294

Back, S., & Guerette, R. T.. (2021). Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, . http://journals.sagepub.com/doi/10.1177/10439862211001628

Baseri, Y., Chouhan, V., & Hafid, A.. (2024). Navigating quantum security risks in networked environments: a comprehensive study of quantum-safe network protocols. https://doi.org/10.1016/j.cose.2024.103883

Bešić, E.. (2020). Intersectionality: a pathway towards inclusive education?. http://link.springer.com/10.1007/s11125-020-09461-6

Bill of Rights Institute. (n.d.). Eli whitney and the cotton gin. https://billofrightsinstitute.org/essays/eli-whitney-and-the-cotton-gin/

Bogna, F., Raineri, A., & Dell, G.. (2020). Critical realism and constructivism: merging research paradigms for a deeper qualitative study. *Qualitative Research in Organizations and Management: An International Journal*, . https://www.emerald.com/insight/content/doi/10.1108/QROM-06-2019-1778/full/html

Bongiorno, J.. (2020). Uncovered tracks: the bloody legacy of canada's railways - canada's national observer: climate news. https://www.nationalobserver.com/2020/12/21/opinion/bloody-legacy-canadas-railways-indigenous-peoples

Bruno, L., & Spano, I.. (2021). Post-quantum encryption and privacy regulation: can the law keep pace with technology?. *European Journal of Privacy Law and Technologies*, . https://heinonline-org.ezproxy.lib.ucalgary.ca/HOL/Page?public=true&handle=hein.journals/ejplt2021&div=8&start_page=72&collection=journals&set_as_cursor=0&men_tab=srchresults

Cain, A. A., Edwards, M. E., & Still, J. D.. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, . https://linkinghub.elsevier.com/retrieve/pii/S2214212618301455

Canadian Centre for Cyber Security. (2022). National cyber threat assessment 2023-2024.

Carley, K. M.. (2020). Social cybersecurity: an emerging science. http://link.springer.com/10.1007/s10588-020-09322-9

Cavoukian, A.. (2011). Privacy by design the 7 foundational principles. https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

CCA. (2023). Quantum potential: expert panel on the responsible adoption of quantum technologies. https://www.cca-reports.ca/wp-content/uploads/2024/03/Quantum-Potential_Full-Report_March-1-2024.pdf

Chai, W.. (2022). What is saas (software as a service)? everything you need to know. https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service

Claassen, J. N., Ward, P. J., Daniell, J., Koks, E. E., Tiggeloven, T., & De Ruiter, M. C.. (2023). A new method to compile global multi-hazard event sets. https://www.nature.com/articles/s41598-023-40400-5

Coccia, M.. (2024). Converging artificial intelligence and quantum technologies: accelerated growth effects in technological evolution. https://www.mdpi.com/2227-7080/12/5/66

Colbert, E.. (2017). Security of cyber-physical systems – CSIAC. https://csiac.org/articles/security-of-cyber-physical-systems/

Congress, U.. (2018). H.r.6227 - 115th congress (2017-2018): an act to provide for a coordinated federal program to accelerate quantum research and development for the economic and national security of the united states. https://www.congress.gov/bill/115th-congress/house-bill/6227

Consortium, P.. (2013). Securing software distribution with digital code signing. https://pkic.org/2013/10/16/securing-software-distribution-with-digital-code-signing/

Corporation., I. B. M.. (2022). The quantum decade: a playbook for achieving awareness, readiness, and advantage.

Council of Canadian Academies. (2023). Council of canadian academies - CCA - quantum potential. https://www.cca-reports.ca/reports/quantum-technologies/

Crenshaw, K.. (1991). Mapping the margins: intersectionality, identity politics, and violence against women of color. https://www.jstor.org/stable/1229039?origin=crossref

Cybereco. (2024). Post-quantum cryptography. https://cybereco.ca/wp-content/uploads/Post-Quantum-Cryptography.pdf

Cybersecurity and Infrastructure Security Agency [CISA]. (2024). Joint statement from FBI and CISA on the people's republic of china (prc) targeting of commercial telecommunications infrastructure - CISA. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

Dali, A., & Lajtha, C.. (2012). ISO 31000 risk management— "the gold standard". http://www.tandfonline.com/doi/abs/10.1080/07366981.2012.682494

de Boer, D.. (2023). Introduction. https://doi.org/10.1093/oso/9780198876809.003.0001

De Wolf, R.. (2017). The potential impact of quantum computers on society. http://link.springer.com/10.1007/s10676-017-9439-z

Dekker, T., & Martin-Bariteau, F.. (2022). Regulating uncertain states: a risk-based policy agenda for quantum technologies. *SSRN Electronic Journal*, . https://www.ssrn.com/abstract=4203758

DelViscio, M. T. A. G. J.. (n.d.). How does a quantum computer work?. https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/

Department of Justice Canada. (1982). The canadian charter of rights and freedoms. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/

DeRose, K.. (2022). Establishing the legal framework to regulate quantum computing technology comments. *Catholic University Journal of Law and Technology*, . https://heinonline.org/HOL/P?h=hein.journals/cconsp31&i=363

Digital, M.. (2024). Steady progress in approaching quantum advantage - mckinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage

digitcert. (n.d.). What is code signing? - digicert FAQ. https://www.digicert.com/faq/code-signing-trust/what-is-code-signing

Douha, N. Y., Renaud, K., Taenaka, Y., & Kadobayashi, Y.. (2023). Smart home cybersecurity awareness and behavioral incentives.

https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2023-0032/full/html

Dupont, B.. (2013). Cybersecurity futures: how can we regulate emergent risks?.

Dupont, B.. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, . https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1691855

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P.. (2022). What can a critical cybersecurity do?. https://academic.oup.com/ips/article/doi/10.1093/ips/olac013/6649355

Eidelman, S., & Crandall, C. S.. (2014). The intuitive traditionalist. https://linkinghub.elsevier.com/retrieve/pii/B9780128002841000023

Establishment, C. S.. (2007). Harmonized threat and risk assessment methodology. https://www.cyber.gc.ca/sites/default/files/cyber/publications/tra-emr-1-e.pdf

European Commission. (2016). European strategy for quantum technology endorsed by 3400 key players - shaping europe's digital future. https://digital-strategy.ec.europa.eu/en/news/european-strategy-quantum-technology-endorsed-3400-key-players

Federal Communications Commission. (2023). FCC adopts updated data breach notification rules to protect consumers - federal communications commission. https://www.fcc.gov/document/fcc-adopts-updated-data-breach-notification-rules-protect-consumers-0

Fiedler, R., & Günther, F.. (2024). Security analysis of signal's PQXDH handshake. https://eprint.iacr.org/2024/702

Flemming, J.. (2023). The future of quantum computing in environmental and health sciences. https://uwaterloo.ca/news/future-quantum-computing-environmental-and-health-sciences

Flöther, F., Murphy, J., Murtha, J., & Sow, D.. (2020). IBM exploring quantum computing use cases for healthcare.

Francis, B.. (2022). Listen: BOA global strategist sees a transition from oil to cleaner energy options and increased u.s.-based manufacturing. https://fortworthreport.org/2022/09/17/listen-boa-global-strategist-sees-a-transition-from-oil-to-cleaner-energy-options-and-increased-u-s-based-manufacturing/

Fussell, S.. (2020). How surveillance has always reinforced racism - WIRED. https://www.wired.com/story/how-surveillance-reinforced-racism/?utm_source=chatgpt.com

Gambetta, J.. (2023). The hardware and software for the era of quantum utility is here. https://www.ibm.com/quantum/blog/quantum-roadmap-2033

Gao, Y. L., Chen, X. B., Chen, Y. L., Sun, Y., Niu, X. X., & Yang, Y. X.. (2018). A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, . https://doi.org/10.1109/ACCESS.2018.2827203

Gidney, C., & Ekerå, M.. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. http://arxiv.org/abs/1905.09749

Global Affairs Canada. (n.d.). A guide to canada's export control list - 2024. https://www.international.gc.ca/trade-commerce/controls-controles/ecl-lec/export_control_list-guide-liste_exportation_controlee_2024.aspx?lang=eng

Government of British Columbia. (2022). Risk management guideline for the b.c. public sector.

Government of Canada. (2023). The canadian critical minerals strategy - from exploration to recycling: powering the green and digital economy for canada and the world.

Government of Canada. (2000). Personal information protection and electronic documents act. https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

Government of Canada, Innovation. (2023). National quantum strategy - home. https://ised-isde.canada.ca/site/national-quantum-strategy/en/overview-canadas-national-quantum-strategy

Graz, J., & Hauert, C.. (2019). Translating technical diplomacy: the participation of civil society organisations in international standardisation. https://www.tandfonline.com/doi/full/10.1080/13600826.2019.1567476

Grover, L. K.. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the {Annual} {ACM} {Symposium} on {Theory} of {Computing}*. https://doi.org/10.1145/237814.237866

Hancock, A.. (2023). The last mile of encrypting the web: 2023 year in review. https://www.eff.org/deeplinks/2023/12/year-review-last-mile-encrypting-web

Hassija, V., Chamola, V., Goyal, A., Kanhere, S. S., & Guizani, N.. (2020). Forthcoming applications of quantum computing: peeking into the future. https://onlinelibrary.wiley.com/doi/10.1049/iet-qtc.2020.0026

HM Government. (2023). National risk register - 2023 edition. https://assets.publishing.service.gov.uk/media/64ca1dfe19f5622669f3c1b1/2023_NATIONAL_RISK_REGISTER_NRR.pdf

Hull, M., Zhang-Kennedy, L., Baig, K., & Chiasson, S.. (2022). Understanding individual differences: factors affecting secure computer behaviour. https://www.tandfonline.com/doi/full/10.1080/0144929X.2021.1977849

Human-Centric Cybersecurity Partnership. (n.d.). Human-centric cybersecurity partnership summer 2024 preliminary report. https://www.hc2p.ca/summerreports

IBM. (n.d.). What is quantum computing? - IBM. https://www.ibm.com/topics/quantum-computing

Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F.. (2021). Systematic and critical review of RSA based public key cryptographic schemes: past and present status. *IEEE Access*,

Innovation, Science and Economic Development Canada. (2023). Canada's national quantum strategy. https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy

Innovation, Science and Economic Development Canada. (2022). Canada's national quantum strategy. https://publications.gc.ca/site/eng/9.914144/publication.html

Innovation, Science and Economic Development Canada. (2023). Canada's national quantum strategy. https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy

Innovation, Science and Economic Development Canada. (2023). Key small business statistics - 2023. https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2023#s4.2

Innovation, Science and Economic Development Canada. Quantum Readiness Working Group [QRWG] (2023). Canadian national quantum-readiness: best practices and guidelines. https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/cfdir-quantum-readiness-best-practices-v03.pdf

Jiang, J., Wang, D., Zhang, G., & Chen, Z.. (2022). Quantum-resistant password-based threshold single-sign-on authentication with updatable server private key. https://link.springer.com/10.1007/978-3-031-17146-8_15

Jovićević, A.. (2021). Concepts between kant and deleuze: from transcendental idealism to transcendental empiricism. https://epochemagazine.org/41/concepts-between-kant-and-deleuze-from-transcendental-idealism-to-transcendental-empiricism/

Jyothi Ahuja, N., & Dutt, S.. (2022). Implications of quantum science on industry 4.0: challenges and opportunities. https://link.springer.com/10.1007/978-3-031-04613-1_6

Kaur, M., & Venegas-Gomez, A.. (2022). Defining the quantum workforce landscape: a review of global quantum education initiatives. https://www.spiedigitallibrary.org/journals/optical-engineering/volume-61/issue-08/081806/Defining-the-quantum-workforce-landscape--a-review-of-global/10.1117/1.OE.61.8.081806.full

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S.. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, . https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab005/6170701

Kelly, S. A. W. W.. (n.d.). The digital divide has become a chasm: here's how we bridge the gap. https://www.cigionline.org/articles/the-digital-divide-has-become-a-chasm-heres-how-we-bridge-the-gap/

Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H.. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. https://www.mdpi.com/2076-3417/13/6/3410

Konkoly-Thege, K., & Jackson, M.. (2022). The legal implications of quantum computing. *American Bar Association Journal*, . https://ezproxy.lib.ucalgary.ca/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Flegal-implications-quantum-computing%2Fdocview%2F2738617000%2Fse-2%3Faccountid%3D9838

Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I. G., Brongersma, M., Quintel, T., Floridi, L., & Laflamme, R.. (2023). Towards responsible quantum technology. *SSRN Electronic Journal*, . https://www.ssrn.com/abstract=4393248

Laboratory, O. R. N.. (2022). Crossing the quantum frontier. https://www.ornl.gov/news/crossing-quantum-frontier

Lalonde, C., & Boiral, O.. (2012). Managing risks through ISO 31000: a critical analysis. http://link.springer.com/10.1057/rm.2012.9

Lambden, S., Laterre, P. F., Levy, M. M., & Francois, B.. (2019). The SOFA score—development, utility and challenges of accurate assessment in clinical trials. https://ccforum.biomedcentral.com/articles/10.1186/s13054-019-2663-7

Laszlo, A., & Krippner, S.. (1998). Systems theories: their origins, foundations, and development. https://linkinghub.elsevier.com/retrieve/pii/S0166411598800174

Lawson, S.. (2013). Beyond cyber-doom: assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics*, . https://www.tandfonline.com/doi/full/10.1080/19331681.2012.759059

Lebowitz, M. J.. (2023). What happens when the packets go away? how the quantum internet will diminish government electronic surveillance programs and change cybersecurity forever. *Boston University Journal of Science and Technology Law*, . https://heinonline.org/HOL/P?h=hein.journals/jstl29&i=39

Ledger, T. Q. R.. (2024). The quantum resistant ledger. https://www.theqrl.org/

Lee, M.. (2023). A framework for assessing vulnerabilities in the quantum computing materials supply chain.

Li, Z., Wang, D., & Morais, E.. (2022). Quantum-safe round-optimal password authentication for mobile devices. https://ieeexplore.ieee.org/document/9272675

Lindsay, J. R.. (2020). Surviving the quantum cryptocalypse.

Liu, Y., Du, D., Xia, Y., Chen, H., Zang, B., & Liang, Z.. (2018). Splitpass: a mutually distrusting two-party password manager. *Journal of Computer Science and Technology*, . https://doi.org/10.1007/s11390-018-1810-y

Liu, Y., Du, D., Xia, Y., Chen, H., Zang, B., & Liang, Z.. (2018). Splitpass: a mutually distrusting two-party password manager. *Journal of Computer Science and Technology*, . https://doi.org/10.1007/s11390-018-1810-y

Luiijf, E., & Klaver, M.. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, . https://linkinghub.elsevier.com/retrieve/pii/S1874548221000585

Maqsood, S., & Chiasson, S.. (2021). Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. https://dl.acm.org/doi/10.1145/3469821

Marshall, J. C.. (2001). The multiple organ dysfunction syndrome.

Mashatan, A., & Turetken, O.. (2020). Preparing for the information security threat from quantum computers. https://doi.org/10.17705/2msqe.00030

Mashatan, A., & Turetken, O.. (2020). Preparing for the information security threat from quantum computers.

Mator, J. D., & Still, J. D.. (2021). Impact of the cyber hygiene intelligence and performance (chip) interface on cyber situation awareness and cyber hygiene. https://link.springer.com/10.1007/978-3-030-90238-4_21

Meitz, A., Sagmeister, P., Langemann, T., & Herwig, C.. (2014). An integrated downstream process development strategy along qbd principles. https://www.mdpi.com/2306-5354/1/4/213

MITRE. (2018). CAPEC - capec-206: signing malicious code (version 3.9). https://capec.mitre.org/data/definitions/206.html

Mosca, M., & Piani, M.. (2022). Quantum threat timeline report 2022.

Mosca, M., & Piani, M.. (2022). QUANTUM THREAT TIMELINE REPORT 2022.

National Institute for Standards and Technology. (2024). NIST cybersecurity framework 2.0: enterprise risk management quick-start guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1303.ipd.pdf

National Institute of Standards and Technology. (2017). Post-quantum cryptography - CSRC - CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography

National Institute of Standards and Technology. (2024). Round 4 submissions: post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions

National Institute of Standards and Technology. (2023). Quantum-readiness: migration to post-quantum cryptography. https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

National Institute of Standards and Technology. (2024). NIST post quantum cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography

Natsheh, A. A., Gbadegeshin, S. A., Rimpiläinen, A., Imamovic-Tokalic, I., & Zambrano, A.. (2015). Identifying the challenges in commercializing high technology: a case study of quantum key distribution technology.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M.. (2020). Holistic cyber hygiene education: accounting for the human factors. https://linkinghub.elsevier.com/retrieve/pii/S0167404820300183

Nili, C., Patterson, T., & Dukatz, C.. (2024). Safeguarding central bank digital currency systems in the post-quantum computing age. https://www.weforum.org/agenda/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/

Nobles, C., & Mcandrew, I.. (2023). The intersectionality of offensive cybersecurity and human factors: a position paper. https://www.sciendo.com/article/10.2478/bsaft-2023-0022

NSF. (2024). Cyber-physical systems (cps). https://new.nsf.gov/funding/opportunities/cyber-physical-systems-cps

Office of the Privacy Commissioner of Canada. (2022). 2022-23 departmental plan. https://

www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2022-2023/dp_2022-23/

Office of the Privacy Commissioner of Canada. (2016). PIPEDA report of findings \#2016-005: joint investigation of ashley madison by the privacy commissioner of canada and the australian privacy commissioner/acting australian information commissioner. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/

Organization, I. S.. (2018). ISO 31000:2018(en) risk management — guidelines. https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

Page, C.. (2022). Ransomware gang caught using microsoft-approved drivers to hack targets. https://techcrunch.com/2022/12/13/cuba-ransomware-microsoft-drivers/

Papamichael, M., Dimopoulos, C., & Boustras, G.. (2024). Performing risk assessment for critical infrastructure protection: an investigation of transnational challenges and human decision-making considerations. https://doi.org/10.1080/23789689.2024.2340368

Parliament of Canada. (n.d.). Government bill (house of commons) C-26 (44-1) - third reading - an act respecting cyber security, amending the telecommunications act and making consequential amendments to other acts - parliament of canada. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/third-reading

Parliament of Canada. (n.d.). Government bill (house of commons) C-26 (44-1) - third reading - an act respecting cyber security, amending the telecommunications act and making consequential amendments to other acts - parliament of canada. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/third-reading

Parliament of Canada. (n.d.). Government bill (house of commons) C-27 (44-1) - first reading - digital charter implementation act, 2022 - parliament of canada. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

Payments Canada. (2022). Central bank digital currency (cbdc): wholesale CBDC global developments - payments. https://www.payments.ca/insights/research/central-bank-digital-currency-cbdc-wholesale-cbdc-global-developments

Perkowitz, S.. (2021). The bias in the machine: facial recognition technology and racial disparities. https://mit-serc.pubpub.org/pub/bias-in-machine/release/1

Pidgeon, N., & O'Leary, M.. (2000). Man-made disasters: why technology and organizations (sometimes) fail. https://linkinghub.elsevier.com/retrieve/pii/S0925753500000047

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D.. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. https://journals.scholarsportal.info/details/14355558/v24i0002/371_lhficaima.xml

Porter, M. E.. (1990). The competitive advantage of nations. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Public Safety Canada. (2021). National cross sector forum 2021-2023 action plan for critical infrastructure. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/2021-ctn-pln-crtcl-nfrstrctr-en.pdf

Public Safety Canada. (2024). National risk profile - a national emergency preparedness and awareness tool. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nrp-pnr/2023-npr-pnr-en.pdf

Qin, Y., Ding, R., Cheng, C., Bindel, N., Pan, Y., & Ding, J.. (2022). Light the signal: optimization of signal leakage attacks against lwe-based key exchange.. https://doi.org/10.1007/978-3-031-17140-6_33.

Quantum and Society. (n.d.). Quantum and society. https://quantsoc.net/

Reuter, A., Abdelmaksoud, A., Boudaoud, K., & Winckler, M.. (2021). Usability of end-to-end encryption in e-mail communication. *Frontiers in Big Data*, . https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2021.568284

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K.. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies.. https://ieeexplore.ieee.org/document/969131/

Roberson, T. M.. (2021). On the social shaping of quantum technologies: an analysis of emerging expectations through grant proposals from 2002–2020. *Minerva*, . https://link.springer.com/10.1007/s11024-021-09438-5

Roberson, T., Leach, J., & Raman, S.. (2021). Talking about public good for the second quantum revolution: analysing quantum technology narratives in the context of national strategies. https://iopscience.iop.org/article/10.1088/2058-9565/abc5ab

Rocheleau, J. N., & Chiasson, S.. (2022). Privacy and safety on social networking sites: autistic and non-autistic teenagers' attitudes and behaviors. https://dl.acm.org/doi/10.1145/3469859

Ruwet, C.. (2011). Towards a democratization of standards development? internal dynamics of ISO in the context of globalization. https://www.degruyter.com/document/doi/10.2202/1940-0004.1140/html

Sachs, J. D., Karim, S. S. A., Aknin, L., Allen, J., Brosbøl, K., Colombo, F., Barron, G. C., Espinosa, M. F., Gaspar, V., Gaviria, A., Haines, A., Hotez, P. J., Koundouri, P., Bascuñán, F. L., Lee, J., Pate, M. A., Ramos, G., Reddy, K. S., Serageldin, I., ..., Michie, S.. (2022). The lancet commission on lessons for the future from the COVID-19 pandemic. https://linkinghub.elsevier.com/retrieve/pii/S0140673622015859

School, Stanford Law and Technology, Stanford Center for Responsible Quantum. (n.d.). Quantum criticality index: understanding critical raw materials supply chains in quantum technologies. https://law.stanford.edu/stanford-center-for-responsible-quantum-technology/projects/quantum-criticality-index/

Serrano, D., Kuppusamy, S. K., Heinrich, B., Fuhr, O., Hunger, D., Ruben, M., & Goldner, P..

(2022). Ultra-narrow optical linewidths in rare-earth molecular crystals. https://www.nature.com/articles/s41586-021-04316-2

Sharma, M.. (2021). China reportedly planning to use quantum computers to decrypt stolen data. https://www.techradar.com/news/china-reportedly-planning-to-use-quantum-computers-to-decrypt-stolen-data

Shor, P.. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th {Annual} {Symposium} on {Foundations} of {Computer} {Science}*. http://ieeexplore.ieee.org/document/365700/

Shor, P. W.. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings - {Annual} {IEEE} {Symposium} on {Foundations} of {Computer} {Science} ({FOCS})*. https://doi.org/10.1109/SFCS.1994.365700

Silberman, D. M.. (2022). Quantum education and pathways: an open-source modifiable presentation to high school and college students. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12213/2641537/Quantum-education-and-pathways--an-open-source-modifiable-presentation/10.1117/12.2641537.full

Simpson, N. P., Mach, K. J., Constable, A., Hess, J., Hogarth, R., Howden, M., Lawrence, J., Lempert, R. J., Muccione, V., Mackey, B., New, M. G., O'Neill, B., Otto, F., Pörtner, H., Reisinger, A., Roberts, D., Schmidt, D. N., Seneviratne, S., Strongin, S., ..., Trisos, C. H.. (2021). A framework for complex climate change risk assessment. https://linkinghub.elsevier.com/retrieve/pii/S2590332221001792

Solenov, D., Brieler, J., & Scherrer, J. F.. (2018). The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6205278/

Stewart, H.. (2011). Normative foundations for reasonable expectations of privacy. In *The {Supreme} {Court} {Law} {Review}: {Osgoode}'s {Annual} {Constitutional} {Cases} {Conference}*. https://digitalcommons.osgoode.yorku.ca/sclr/vol54/iss1/12

Supreme Court of Canada. (2015). Goodwin v. british columbia (superintendent of motor vehicles) - SCC cases. https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/15550/index.do

Supreme Court of Canada. (2017). R. v. marakah - SCC cases. https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/16896/index.do

Supreme Court of Canada. (2024). R. v. bykovets - SCC cases. https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/20302/index.do

Szikora, P., & Lazányi, K.. (2022). The end of encryption? – the era of quantum computers.

Tang, M.. (2022). The challenge of the cloud: between transnational capitalism and data sovereignty. https://www.tandfonline.com/doi/full/10.1080/1369118X.2022.2128598

Temoshok, D., Fenton, J., Choong, Y., Lefkovitz, N., Regenscheid, A., & Richer, J.. (2024). Digital identity guidelines: authentication and authenticator management.

Tosh, D., Galindo, O., Kreinovich, V., & Kosheleva, O.. (2020). Towards security of cyber-physical systems using quantum computing algorithms. In *2020 {IEEE} 15th {International} {Conference} of {System} of {Systems} {Engineering} ({SoSE})*. https://ieeexplore.ieee.org/document/9130525

Tosh, D., Galindo, O., Kreinovich, V., & Kosheleva, O.. (2020). Towards security of cyber-physical systems using quantum computing algorithms. In *2020 {IEEE} 15th {International} {Conference} of {System} of {Systems} {Engineering} ({SoSE})*. https://ieeexplore.ieee.org/document/9130525/

Treasury Board of Canada Secretariat. (2016). Guide to integrated risk management. https://www.canada.ca/en/treasury-board-secretariat/corporate/risk-management/guide-integrated-risk-management.html

Tsatsou, P.. (2022). Vulnerable people's digital inclusion: intersectionality patterns and associated lessons. https://www.tandfonline.com/doi/full/10.1080/1369118X.2021.1873402

Tsatsou, P.. (2022). Vulnerable people's digital inclusion: intersectionality patterns and associated lessons. https://doi.org/10.1080/1369118X.2021.1873402

US Department of Health and Human Services. (2020). SOFA score: what it is and how to use it in triage.

Valinejad, J., & Mili, L.. (2023). Cyber–physical–social model of community resilience by considering critical infrastructure interdependencies. *IEEE Internet of Things Journal*, . https://ieeexplore.ieee.org/document/10129123/

van der Sloot, B., & van Schendel, S.. (2024). *The boundaries of data*. Amsterdam University Press. https://www.aup.nl/en/book/9789463729192/the-boundaries-of-data

Van Steen, T., Norris, E., Atha, K., & Joinson, A.. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity*, . https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyaa019/6032830

Waddell, M.. (2024). Human factors in cybersecurity: designing an effective cybersecurity education program for healthcare staff. http://journals.sagepub.com/doi/10.1177/08404704231196137

Wang, Q., Wang, D., Cheng, C., & He, D.. (2021). Quantum2fa: efficient quantum-resistant two-factor authentication scheme for mobile devices. https://ieeexplore.ieee.org/abstract/document/9623421?casa_token=-LhkWXbBkfcAAAAA:dm9JjmSnHnBHVeiG_3qps9JfmTvW4pTzN2jmKNC6avgRb3oQJZblVzNdbc5HbiT-uSsCGo45kw)

Witt, S.. (2022). The world-changing race to develop the quantum computer. https://www.newyorker.com/magazine/2022/12/19/the-world-changing-race-to-develop-the-quantum-computer

Wolbring, G.. (2022). Auditing the 'social' of quantum technologies: a scoping review. https://www.mdpi.com/2075-4698/12/2/41

Ying, M.. (2010). Quantum computation, quantum theory and AI. https://linkinghub.elsevier.com/retrieve/pii/S0004370209001398

Zhang, L., Miranskyy, A., Rjaibi, W., Stager, G., Gray, M., & Peck, J.. (2023). Making existing software quantum safe: a case study on IBM db2. *Information and Software Technology*, . http://arxiv.org/abs/2110.08661

Zhang-Kennedy, L., & Chiasson, S.. (2022). A systematic review of multimedia tools for cybersecurity awareness and education. https://dl.acm.org/doi/10.1145/3427920

Human-Centric
Cybersecurity
Partnership