Quantum Risk Assessment

Project Proposal

Fareen Lavji
Innovation, Science, and Economic Development Canada

EXECUTIVE SUMMARY

"*The Canadian Forum for Digital Infrastructure Resilience (CFDIR) is a voluntary, consensus-based and action-oriented public-private collaboration formed to enhance the resilience of the Canadian critical digital infrastructure, resulting in a trusted digital economy for Canadians and a thriving cyber security industry*." [2]

CFDIR's Quantum-Readiness working group, currently chaired by Dr. Michelle Mosca, has identified that one challenge facing decision makers, in the quantum resilience space, is that there is no consensus on what is precisely the timeline of the emerging quantum threat to cryptography. This is an issue because current risk assessment methodologies calculate risks in the present which is inherently a problem as most risks may (or may not) be proven in the future. Additionally, there is no consensus on what is precisely the correct timeline of quantum innovation.

The Quantum Risk Assessment project, proposed in this paper, is envisioned to be a one year undergraduate project, including interactions with key stakeholders in the industry. The goal of this project is to create a hybrid risk assessment that accounts for time as a variable. In doing this, it could facilitate critical infrastructure owners and other bodies of operation to plan for mitigating risks in parallel to the speed of innovation.

GLOSSARY

Asset Value	Monetary value assigned to a collection of assets
Countermeasure	Planned procedures to reduce the effects of risks in infrastructures
Likelihood	A numerical value assigned to the probability of an event occurring
Logarithmic Function	Inverse of exponential functions that curve based on specified degrees
Logical Reasoning	Use of abstraction to reason mathematically, complex issues and/or events
Quantum Computing	A new and emerging form of computation that relies on quantum states
Quantum Resilience	A new and emerging school of thought to prepare for the increasingly apparent threat of commercialization and large scale use of quantum computation
Rational Function	A fractional function that uses polynomials in the numerator and denominator
Risk Assessment	A standard project managerial procedure used to determine risks of events and/or projects
Threat	A numerical value assigned to the magnitude of threat
Vulnerability	A numerical value assigned to the potential for an entity to fall under threat

ABBREVIATIONS

CFDIR	Canadian Forum for Digital Infrastructure Resilience
CI	Critical Infrastructure
ICT	Information and Communication Technology
NIST	National Institute of Standards and Technology
QRWG	Quantum-Resilience Working Group
RA	Risk Assessment

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

1.1 PURPOSE

Current *Risk Assessment* (RA) methodologies do not factor future risks, the Quantum Risk Assessment Project works to fill that gap.

1.2 UTILITY

Quantum Computing is not widely understood to be a threat in current times. However, with increased use and commercialization, future risks need to be highlighted. And to prepare for future risks, organizations and bodies need to account for the time it can take to migrate their infrastructure to be *Quantum Resilient*. This *RA* can be used to account for the relation between preparing for new innovation and the speed of innovation.

1.3 NOVELTY

The Quantum RA is unique in the fact that it introduces time as a variable to account for how long it can take to migrate an infrastructure in parallel to the speed of innovation.

1.4 INGENUITY

The main attribute for this project is that it incorporates time as a variable to highlight the magnitude of the threat in relation to current circumstances.

2 SCOPE

There are vast libraries of RA methodologies that can be applied to numerous scenarios. However, generally, RA methodologies can be divided into the following processes [1]:

1. Preparation
2. Conduct
    A. Identify
    B. Determine
3. Communicate and Share
4. Maintain

Figure 1: General Risk Assessment [1]

The focus of this project is to enhance the conduct stage, particularly, determining the risk (step 2.B.) in a Quantum RA.

3 BACKGROUND

The Canadian Forum for Digital Infrastructure Resilience (CFDIR) is a voluntary, consensus-based and action-oriented public-private collaboration formed to enhance the resilience of the Canadian critical digital infrastructure, resulting in a trusted digital economy for Canadians and a thriving cyber security industry. [2]

CFDIR operates primarily through working groups, one of them being Quantum-Readiness. Quantum-readiness is a school of thought dedicated to updating the [Canadian] *information and communication* (ICT) infrastructure to be prepared for commercialization of *quantum computing* and the risks they can bring. Dr. Michele Mosca, the current Chair for the *Quantum-Readiness Working Group* (QRWG), in collaboration with members of the QRWG, independently, and other bodies of operation, has prepared several publications.

One of the challenges, that the QRWG is facing is bringing to light the reality of the imminent threat *quantum computing* will bring. Many interested parties do not consider *quantum computing* as a *threat that has to dealt with in the near future,* as RA methodologies do not account for future risks which are not priorities for many organizations and bodies.

If a dynamic risk assessment methodology were to be created that could be implemented for quantum risk assessments as well as other future risks, it could vastly increase the applicability of RAs to future threats and, correspondingly, could help *critical infrastructures* (CI) account for future risks and plan accordingly to migrate to a more resilient future.

4 PROJECT DESCRIPTION

4.1 MOSCA'S THEOREM AND THREAT ESTIMATION

Foreseeing the threat of the future, Dr. Michele Mosca is one of the many global champions, advocating for the importance of quantum-readiness. In helping for preparations, many white papers and reports have been published with timelines and formulas. In collaboration with John Mulholland and through the Global Risk Institute, Dr. Mosca published *Mosca's Theorem* [3], which is a simple formula, highlighting the importance of starting migration as early as possible for quantum readiness.

$$x + y > z$$

$x = lifetime\ of\ assets$

$y = time\ required\ to\ transform\ infrastructure$

$z = time\ to\ quantum\ reality$

Equation 1: Mosca's Theorem [3]

As can be observed by Mosca's theorem, 3 variables are identified: **lifetime of all assets** that a body of operation houses; **time** required to transform all assets to be quantum resilient; **estimated time** to quantum reality and large scale use. Furthermore, this equation depicts that if the sum of the **lifetime of an entities assets** and the **time required to migrate the infrastructure** of said entity is greater than the **time to quantum reality** (i.e., commercialization, large-scale use, etc.), then the entity should be concerned.

To derive the value of z (i.e., **time to quantum reality**), the Global Risk Institute also published Dr. Mosca and Dr. Marco Piani's Quantum Threat Estimation report[1]. This 2020 survey reflected the opinions of 44 industry experts on the likelihood of significant quantum threats over time.

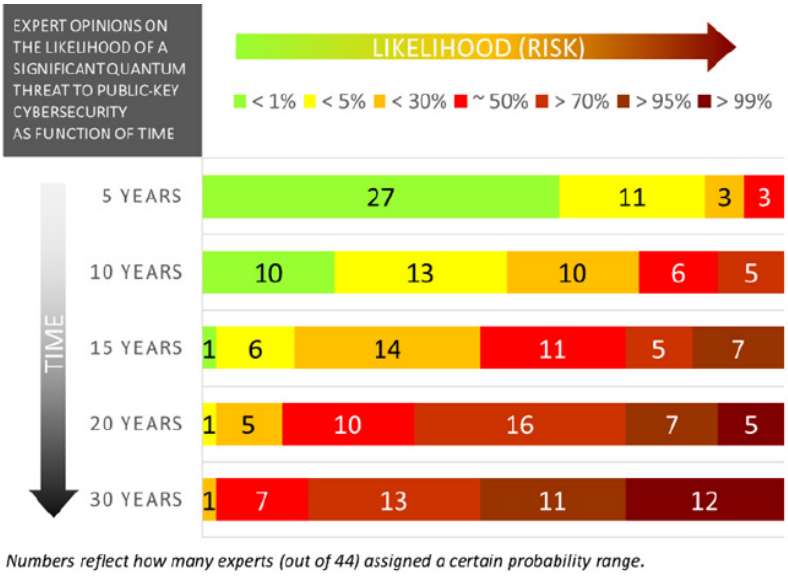

Figure 2: Chart of expert opinions on the likelihood of a significant quantum threat. [4]

Based on individual expertise and tolerances for risk, the information in Figure 2 can be used to select a value for 'z' (i.e., the time to quantum realty).

[1] See Figure 2.

4.2 Preliminary Research

As mentioned within the scope of this project, there are numerous ways to conduct RAs. Consequently, there are numerous ways to determine the magnitude of risks for itemized *threats* and *vulnerabilities*. However, RA calculations can be divided into 2 classifications:

1. Qualitative
2. Quantitative

Qualitative RAs depend on an RA tables similar to the one below:

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 1: Table I-2 from SP800-30 showcasing Assessment Scale – Level of Risk [1]

Quantitative RAs use a formula that relies upon basic *logical reasoning* like adding or multiplying all your "negative" variables (i.e., *threat*, *vulnerability*, etc.) and subtracting or dividing positive *countermeasures* to the corresponding results. Equation 2 and 3 are general reflections of the equations that can be seen throughout Quantitative RAs:

$$Risk = Threat \times Vulnerability \times Asset\ Value$$

Equation 2: General quantitative risk calculation

$$Risk = \left(\frac{Vulnerability \times Threat}{CounterMeasure}\right) Asset\ Value$$

Equation 3: Risk formula that accounts for countermeasures

Qualitative RAs account for *likelihood* which is inherently a problem with the quantum RAs, given that the likelihood of *threat* at present time is null. Because of this, it would be beneficial to create a hybrid RA with an additional formulation that derives the likelihood. This can help calculate for future risks.

4.3 PROPOSED RISK CALCULATION

To highlight the importance of future risks, it is important to introduce time as variable and curve up the scale of risk based on time to migration for resilience. This can be done by combining and testing 3 types of functions and/or expressions:

1. *Logical Reasoning* Refer to Equation 2 and 3
2. *Logarithmic*

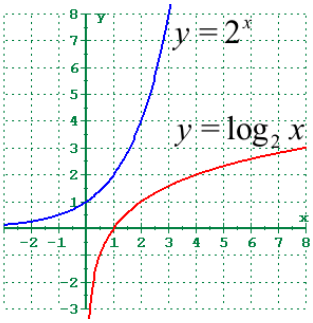

Figure 3: Sample logarithmic graph

3. *Rational*

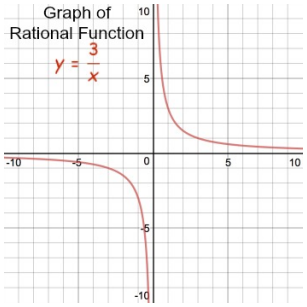

Figure 4: Sample rational graph

The strategy would be to produce an equation that creates a threat-multiplier variable based on the user's tolerance level to the risks reflected in the Mosca-Piani 2021 quantum threat timeline report [4]. This variable would then be used as a coefficient in the hybrid Quantum Risk Assessment.

4.4 PROJECT PLAN

As outlined in the Project Calendar[2], the research will be divided into 4 phases:

1. Prototype
    a. This phase will look to do some further research and put together a sample RA Guide for IT systems
2. Alpha
    a. During this phase, the RA Guide can be tested in either of 2 ways:
        i. Distribution of the RA Guide to a sample of the key stakeholders invested in the emerging quantum reality
        ii. Creating a program that can produce large datasets for testing and verifying
    b. This phase will focus on reefing the prototype based on feedback from the tests
3. Beta
    a. Following the alpha phase, the refined RA Guide will be distributed to key stakeholders as outlined in **Step 2.a.i**.
4. Deploy
    a. During deployment, the RA guide will be polished and ready for publications for the Canadian CIs benefit

b.

5 CONCLUSION

The Quantum RA is a dynamic RA that has potential to revolutionize current RA methodologies by allowing future thinkers to prepare for innovation in parallel to the velocity of innovation. In this particular case, the Quantum RA is a one year project that will enable key stakeholders to migrate their current cryptographic architectures to a *quantum resilient* infrastructure by integrating time as a prime variable in the Assessment process.

[2] Appendix 7.1

6 APPENDICES

6.1 REFERENCES

[1] National Institute of Standards and Technology (NIST), "NIST SP 800-30," 21 April 2021. [Online]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-30. [Accessed 19 11 2021].

[2] Innovation, Science, and Economic Development Canada, "Canadian Forum for Digital Infrastructure Resilience," 01 10 2020. [Online]. Available: https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11618.html. [Accessed 19 11 2021].

[3] J. M. Dr. Michele Mosca, "A Methodology for Quantum Risk Assessment," 5 January 2017. [Online]. Available: https://globalriskinstitute.org/publications/3423-2/. [Accessed 19 11 2021].

[4] D. M. P. Dr. Michele Mosca, "Quantum Threat Timeline Report 2020," 27 January 2021. [Online]. Available: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/. [Accessed 19 11 2021].

6.2 PROJECT CALENDAR

Phase	Stage	Item	Deliverables	Timeline
1	**Prototype**	Prototype Package	✓ Research ✓ Methodology ✓ Application Guide	Wk 01 - 03
		Risk Assessment Guide, D1	✓ Draft Publication	Wk 03 - 05
		Progress Report, P1	✓ Prototype Package ✓ RA Guide, D1 ✓ Retrospective	Wk 06
2	**Alpha**	Alpha Package	✓ Data Points ✓ Questions ✓ Analysis Guide	Wk 07 - 08
		Questionnaire, FGS1	✓ Questions ✓ Answer Guide	Wk 09
		Results, FGS1	✓ Raw Results ✓ Aggregated ✓ Analysis	Wk 10 - 21
		Progress Report, P2	✓ Alpha Package ✓ Results, FGS1 ✓ Retrospective	Wk 22
3	**Beta**	Beta Package	✓ RA Guide, D1.2 ✓ Data Points ✓ Questions ✓ Analysis Guide	Wk 23 - 25
		Risk Assessment Guide, D2	✓ Quantitative ✓ Qualitative ✓ Suggested updates and improvements	Wk 26 - 28

		Questionnaire, FGS2	✓ Questions ✓ Answer Guide	Wk 29
		Results, FGS2	✓ Raw Results ✓ Aggregated ✓ Analysis	Wk 30 - 41
		Progress Report, P3	✓ Alpha Package ✓ Results, FGS1 ✓ Retrospective	Wk 42
4	**Deploy**	Risk Assessment Guide, D3	✓ Quantitative ✓ Qualitative ✓ Suggested updates and improvements	Wk 43 - 45
		Report, Final	✓ Compile Progress Reports ✓ Compile stage packages ✓ Retrospective	Wk 46 - 47
		Presentation, Final	✓ PowerPoint ✓ Handout	Wk 48

Table 2: Timeline based on capacity of undergraduate student working part-time