Analyzing Dependencies among Challenges for Quantum-safe Transition

Kong, Ini; Janssen, Marijn; Bharosa, Nitesh

Publication date
2023

Document Version
Final published version

Published in
CEUR Workshop Proceedings

Analyzing Dependencies among Challenges for Quantum-safe Transition

Ini Kong [1], Marijn. Janssen [1] and Nitesh. Bharosa [1]

[1] *Delft University of Technology, Delft, Jaffalaan 5, 2628 BX Delf, The Netherlands*

Abstract

The quantum computing-based threats call for a critical information infrastructure to modify widely used cryptographic algorithms to ones that are quantum-safe (QS). Yet, little scholarly research has been undertaken to study QS transition, and the guidance to prepare for socio-technical predicaments of the transition falls short. To address the gaps, the paper aims to determine the contextual interaction between QS transition challenges and classify these challenges into driving power and dependency power. In doing so, we use an integrated Interpretive Structural Modelling (ISM)-Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) approach. The results of ISM-MICMAC analysis indicate that the dominant challenges that organizations need to prioritize are establishing a clear QS transition governance and collaborations in the ecosystem. The findings show that it is crucial for organizations to understand the ecosystem making up the critical information infrastructure they are operating in and collaboratively navigate the action approaches for the QS transition. This also implies that preparation for the QS transition not only includes developing QS solution standards but also requires well-defined roles and responsibilities for various actors in the ecosystem.

Keywords

Quantum-safe transition, Transition challenges, ISM MICMAC analysis

1 Introduction

We now live in a world in which nearly everything is connected to everything else [1, 2]. Information has become the most important building block of our societies, and maintaining the secure transaction of information has become a necessity. Likewise, critical information infrastructure for governments plays an important role in maintaining vital public services for individuals and organizations. The secure functioning of critical information infrastructure not only forms the backbone of a nation's security but also maintains public safety [3, 4].

While many of these services provided by critical information infrastructure depend on today's widely used cryptographic algorithms, we are now entering an era where the infrastructure may no longer be protected. The computation power of quantum computers can potentially break the entire foundational cryptographic layers that information architectures depend on [5, 6]. Although there is no large-scale quantum computer available at the time of writing, information that requires long-term security can still be harvested, stored now, and decrypted later [7-9].

The topic of Quantum-safe (QS) transition is relatively new in the field of Information Systems. In order to safeguard the critical information infrastructure, current cryptographic algorithms need to be modified with ones that are quantum-safe (QS). The National Institute for Standards and Technology (NIST) is currently standardizing QS algorithms using Post Quantum Cryptography (PQC) [7, 10, 11]. Although the development has been ongoing since 2016, substituting these QS algorithms in the current infrastructures with a simple drop-in approach may not be feasible [12, 13].

Due to various use cases and multiple actors involved in critical information infrastructure, QS transition remains complex, and organizations may need to consider all aspects of social-technical predicaments [7, 14-20]. However, there is a void in the literature about the relationship between QS

EGOV-CeDEM-EPart2023, September 05-07, Corvinus University of Budapest, Hungary
EMAIL: i.kong@tudelft.nl (I. Kong); m.f.w.h.a.janssen@tudelft.nl (M.Janssen); n.bharosa@tudelft.nl (N.Bharosa)
ORCID: 0000-0002-4472-8162 (I. Kong); 0000-0001-6211-8790 (M. Janssen); 0000-0002-3919-6413 (N.Bharosa)

transition challenges and how significant they may be to each other in realizing QS transition. To address the gaps in the literature, a research question has been formulated:

RQ. What are the relationships between challenges toward QS transition?

Understanding the relationship between challenges will help us to identify which challenges should be tackled first to transition toward QS. We use the list of QS transition challenges obtained from both literature and expert opinions as input for an Integrated Interpretive Structural Modelling (ISM)-Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) approach. The paper provides the following contribution: i) to discover contextual relationships between QS transition challenges, ii) to develop a hierarchical structural model of QS transition challenges, iii) to identify QS transition challenges that can be tackled first, and iv) to suggest areas for further research.

The paper is structured as follows: section two provides background information on Public Key Infrastructure (PKI) ecosystem and a list of QS transition challenges. Section three discusses the research methodology and provides an overview of the integrated Interpretive Structural Modelling (ISM)-Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) approach. Section four presents data analysis and results of the integrated ISM-MICMAC approach, followed by discussions in section five. The paper concludes in section six with an overview of limitations and directions for future research.

2 Background

2.1 Public Key Infrastructure Ecosystem

Critical information infrastructure plays an important role in providing digital transactions and communication [3, 4]. Notably, Public Key Infrastructure (PKI) ensures the security of these services and also supports platforms of other critical infrastructure, including yet not limited to, finance, healthcare, defense, or national government. By managing identities of users and encryption of information over networks, the security framework of PKI provides a secure environment for individuals, businesses, and government agencies to access information on applications and connected devices [21-23].

Although this paper does not rush to classify the theoretical stands of the term *ecosystem*, we use the definition of *ecosystem* proposed by Adner [24] to describe the interdependencies in the PKI. The term is defined as "t*he alignment structure of the multilateral set of partners that need to interact in order for a focal value proposition to materialize"*[24]. The following definition meets the description of the PKI ecosystem in four ways: 1. Multilateral set of actors have roles they play in the PKI 2. Actors need to interact with each other to perform configuration of activities underlying technical interdependencies of PKI 3. Cryptographic algorithms that are used in PKI need to maintain interoperability and backward compatibility, and 4. The security framework of PKIs has a value proposition to deliver secure digital transactions to its users.

In the context of the Dutch government, governmental PKIs authenticate the identities of users, secure web access and information sharing, and allow digital communications [25]. One of the largest information communication technology (ICT) service providers for the government called SSC-ICT ensures digital means of public services via emails, websites, and other data exchanges [25, 26]. Aside from SSC-ICT maintaining the security of the national government across seven ministries, one of the PKIs in the public sector known as PKIoverheid manages electronic identities of users with PKIo certificates for data exchange systems (e.g. eHerkenning, MedMij, Digikoppeling, and Digipoort) [25].

The Ministry of the Interior and Kingdom Relations (BZK) makes decisions regarding policy and strategy for PKIoverheid, and Logius acts as Policy Authority (PA) managing the infrastructure [27-29]. The external organizations that provide PKIoverheid-related services and products are in compliance with international and EU regulations as well as the Programme of Requirement (PoR) [28]. The standardization bodies such as the National Institute of Standards and Technology (NIST), and European Standard Organizations (ESOs) also have an influence on PKI standards [28]. The user of

such governmental PKIs includes Tax Authority, Customs, Food, and Consumer Product Safety Authority, the Dutch Bank, and other ministries [25].

For QS transition, modifying the cryptographic primitives in governmental PKIs is complex and may need to consider both socio-technical predicaments [15, 19]. PKI is considered as installed system with a set of roles, security policies, encryption mechanisms and procedures [7, 30, 31, 27, 28]. From standardization bodies, regulatory bodies, PKI users to external experts that include service providers, software companies and hardware vendors, many levels of actors that are involved in facilitating PKI systems and delivering PKI-managed services may need to be part of the transition [14-16, 19, 20]. While QS solutions continue to remain undecided, guidance to prepare for the transition falls short and organizations are left with unclear steps for QS transition.

2.2 List of QS Transition Challenges

The QS Transition Challenges are categorized into three different contexts: Technological, Organizational, and Ecosystem Context [32, 33]. Although Technology-Organization-Environment (TOE) framework has been initially used to cluster the QS transition challenges, the term environment has been revised with the term ecosystem to better address challenges that may arise in the context of QS transition. *Error! Reference source not found.* provides an overview of QS transition challenges that have been used as input for ISM-MICMAC approach.

3 Research Methodology

3.1 ISM-MICMAC

In order to examine the contextual relationships among QS transition challenges, we chose an integrated Interpretive Structural Modelling (ISM)-Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) approach. The ISM is a methodology of systemic structuring modelling introduced by Warfield [34], which can be applied when identifying relationships among factors [34]. A set of factors in complex issues are structured into a comprehensive systemic hierarchical model [35, 36]. The MICMAC analysis validates the results obtained from ISM and is introduced by Godet [37] to illustrate the relationship between the factors according to their driving power and dependence power using four categories: autonomous, dependent, linkage, and independent [38, 39, 37, 35]. While ISM can analyze the interrelationships between the factors that influence the system, the MICMAC classifies factors based on driving power and dependence power.

3.2 Expert Opinion

Semi-structured Interviews: The aim of the interviews was to refine the list of QS transition challenges that were previously identified in the literature, *Challenges in the Transition towards a Quantum-safe Government [15]*. The interviews were conducted in the form of semi-structured interviews with experts from industry and government. The selected experts were contacted via emails, and all experts had relevant work experience with PKI systems and had prior knowledge of organizational and/or technical challenges on QS transition. After 12 expert interviews, the list of 15 QS transition challenges was derived as an input for ISM-MICMAC approach. ***Table 1*** shows the list of experts that participated in the interviews.

Workshop: In order to collect the data for Structural Self-Interaction Matrix (SSIM), a workshop was organized in January 2023. Since the workshop provides an opportunity for practitioners to examine the context of the study and share their insights, we invited an expert who maintains the security of critical information infrastructure across Dutch ministries. The selected expert has a prior technical background and holds relevant knowledge and experience from both industry and government. The expert is also familiar with the topic of QS transition and the challenges regarding security strategy, policy, and regulations. Due to the decentralized nature of IT infrastructure in the Dutch government,

we saw that inviting expert who is affiliated with the government PKIs among ministries would help us understand the QS transition challenges among ministries.

Table 1. *List of Experts*

Expert #	Role	Organization
1	Chief Architect	Government Agency
2	Information Sharing Architect	Bank
3	Change Manager	Government Agency
4	Policy Officer	Government Agency
5	Strategic Advisor	Research Institute
6	Chief Technology Officer	Service Provider
7	Architect	Tax Office
8	Cryptographer	Research Institute
9	Policy Coordinator	Government Agency
10	General Manager	Software Company
11	Software Developer	Software Company
12	Vice President of Operations	Service Provider

4 Data Analysis and Results of ISM-MICMAC

This section explains the detailed process of data analysis and the results of the ISM-MICMAC approach.

4.1 Data Analysis of ISM-MICMAC

The steps used in the data analysis of ISM-MICMAC are described below in relation to the topic of this paper.

Step 1: Identify and finalize the list of factors that will be used as input for the ISM-MICMAC approach. The list of QS transition challenges generated by the literature review and expert interviews is shown in **Appendix *1***.

Step 2: Develop Structural Self-Interaction Matrix (SSIM) to collect data on contextual relationships between the list of QS transition challenges.

Step 3: Examine the contextual relationship between any two factors (i and j) and fill out the SSIM. Start from a yellow box (C1, C2) and indicate one of the four symbols below to represent the relationship between factors.

V: Challenge i will influence Challenge j
A: Challenge j will influence Challenge i
X: Challenge i and Challenge j will influence each other
O: Challenge i and Challenge j are not related

Step 4: Establish Initial Reachability Matrix (IRM) from the SSIM matrix. IRM is a binary matrix with 0's and 1's that is derived in accordance to four symbols following the rules for the substitution.

If the (i,j) in the SSIM is V, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 0
If the (i,j) in the SSIM is A, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 1
If the (i,j) in the SSIM is X, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 1
If the (i,j) in the SSIM is O, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 0

Step 5: Test the IRM for transitivity and derive the Final Reachability Matrix (FRM). The transitivity is incorporated to fill the gap and 1* entries are indicated to show the changed relationships for the final reachability matrix. **Table 2** shows the FRM that is revised from the IRM in accordance with the transitivity. The changes are highlighted in grey boxes and are indicated with 1* entries

Concept of Transitivity: If factor A influences factor B, and factor B influences factor C, then factor A also influences factor C. If there was no initial relationship between factor A and factor C in IRM, then the concept of transitivity is achieved between factor A and factor C, and 1* entry is indicated in the FRM.

Table 2. *Final Reachability Matrix*

Structural Self-Interactive Matrix (SSIM)			j													
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints	C1	1	1*	1*	1*	1*	0	1	1	1*	1*	1*	0	1	1*	1*
	No Availability of QS Standardization	C2	1*	1	1*	1	1	1*	1*	1	1*	1*	1	1*	1*	1	1
	No QS Standards & Selection	C3	1	1	1	1	1	1*	1*	1	1*	1	1*	1*	1	1	1
	No Reliable & Secure QS Solutions	C4	1	1	1	1	1	1*	1*	1	1	1*	1*	1*	1*	1	1
	No Availability of QS Hardware & Software	C5	1	1	1*	1	1	1	1*	1	1*	1*	1*	1	1*	1*	1
	Knowledge Needs within Organizations	C6	1	1	1	1	1	1	1	1	1	1	1*	1*	0	1*	1*
	Lack of Urgency within Organizations	C7	1*	1	1	1	1	1*	1	1*	1	1	1*	1*	0	1*	1*
	No Business Case for Organizations	C8	1*	1	1*	1*	1*	1*	1	1	1	1	1	1*	1*	1*	1
	Lack of Technical Skills & Qualified Personnel	C9	1*	1	1	1	1	1*	0	1*	1	1	1*	1	1*	1*	1
	Unclear QS Governance within Organizations	C10	1*	1	1*	1	1	1*	0	1*	1	1	1*	1*	0	1*	1*
	Lack of Urgency in the Ecosystem	C11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Unclear QS Governance in the Ecosystem	C12	1	1	1	1	1	1*	1*	1*	1*	1	1	1	1	1	1
	Lack of Collaboration in the Ecosystem	C13	1	1	1	1	1	1*	1	1	1*	1	1	1	1	1	1
	Lack of Policy & Regulations for QS Solutions	C14	1	1	1	1	1	1	1	1	1	1	1	1	1*	1	1
	Complex Technological Interdependency in the Ecosystem	C15	1	1	1	1	1	1*	1*	1	1*	1	1*	1	1	1	1

Step 7: Obtain a reachability matrix with reachability set and antecedent set from the entries in rows and columns in FRM. E.g. In the reachability set, factors in the row that are affected by factor C1 are identified. In the antecedent set, factors in the column that are affecting factor C1 are identified. After the reachability set and antecedent set are determined, the intersection set is derived from the list of factors from the intersection of these sets.

Step 8: Once the reachability matrix is determined in Step 7, Step 8 is taken to determine the level of each QS transition challenge. Partition the reachability matrix and classify the FRM into various levels. The top-level factors (L1) include those factors that will be led by other factors in the lower level (L2, L3.. etc.). Once the top-level factor is identified, it is removed from consideration. Then, the same process is repeated to find out the factors in the next level. This process continues until the level of each factor is found. **Table 3** shows different levels for QS transition challenges.

Table 3. *Levels for QS Transition Challenges*

Level	Challenges	
Level 1	Legacy System Constraints	C1
	Unclear QS Governance within Organizations	C10
	Lack of Technical Skills & Qualified Personnel	C9
Level 2	Knowledge Needs within Organizations	C6
	Lack of Urgency within Organizations	C7
Level 3	No Availability of QS Standardization	C2
	No QS Standards & Selection	C3
	No Reliable & Secure QS Solutions	C4
	No Availability of QS Hardware & Software	C5
	Knowledge Needs within Organizations	C6
	Lack of Urgency within Organizations	C7
	No Business Case for Organizations	C8
	Lack of Urgency in the Ecosystem	C11
	Lack of Policy & Regulations for QS solutions	C14
	Complex Technological Interdependency in the Ecosystem	C15
Level 4	Unclear QS Governance in the Ecosystem	C12
	Lack of Collaboration in the Ecosystem	C13

Step 9: Organize the ISM-based hierarchy factors using different levels of a partition obtained in Step 7. Develop a visual representation of the ISM-based hierarchy model. The result of the ISM-based hierarchy for QS transition is shown in ***Figure 2***.

Step 10: Analyze the FRM obtained in Step 5 and calculate the summation of rows and columns based on their driving and dependence power. Table 4 shows the summation of driving power and dependence power of QS transition challenges.

Table 4. *Summation of Driving Power & Dependence Power*

Structural Self-Interactive Matrix (SSIM)			j														Driving Power
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	
i	Legacy System Constraints	C1	1	1*	1*	1*	1*	0	1	1	1*	1*	1*	0	1	1*	1*	13
	No Availability of QS Standardization	C2	1*	1	1*	1	1	1*	1*	1	1*	1*	1	1*	1*	1	1	15
	No QS Standards & Selection	C3	1	1	1	1	1	1*	1*	1	1*	1	1*	1*	1	1	1	15
	No Reliable & Secure QS Solutions	C4	1	1	1	1	1	1*	1*	1	1	1*	1*	1*	1*	1	1	15
	No Availability of QS Hardware & Software	C5	1	1	1*	1	1	1	1*	1	1*	1*	1*	1	1*	1*	1	15
	Knowledge Needs within Organizations	C6	1	1	1	1	1	1	1	1	1	1	1*	1*	0	1*	1*	14
	Lack of Urgency within Organizations	C7	1*	1	1	1	1	1*	1	1*	1	1	1*	1*	0	1*	1*	14
	No Business Case for Organizations	C8	1*	1	1*	1*	1*	1*	1	1	1	1	1	1*	1*	1*	1	15
	Lack of Technical Skills & Qualified Personnel	C9	1*	1	1	1	1	1*	0	1*	1	1	1*	1	1*	1*	1	14
	Unclear QS Governance within Organizations	C10	1*	1	1*	1	1	1*	0	1*	1	1	1*	1*	0	1*	1*	13
	Lack of Urgency in the *Ecosystem*	C11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
	Unclear QS Governance in the *Ecosystem*	C12	1	1	1	1	1	1*	1*	1*	1*	1	1	1	1	1	1	15
	Lack of Collaboration in the *Ecosystem*	C13	1	1	1	1	1	1*	1	1	1*	1	1	1	1	1	1	15
	Lack of Policy & Regulations for QS solutions	C14	1	1	1	1	1	1	1	1	1	1	1	1	1*	1	1	15
	Complex Technological Interdependency in the *Ecosystem*	C15	1	1	1	1	1	1*	1*	1	1*	1	1*	1	1	1	1	15
Dependence Power			15	15	15	15	15	14	13	15	15	15	15	14	12	15	15	

Step 11: Classify the factors in a driving and dependence power diagram in accordance with the summation of driving power and dependence power obtained in Step 9. Find out which of the four quadrants each factor belongs to. There are four quadrants in the driving and dependence power diagram:

Autonomous: Factors that have weak drive power and weak dependence power.
Dependent: Factors that have weak drive power but strong dependence power.
Linkage: Factors that have strong drive power as well as strong dependence power.
Independent: Factors that have strong drive power but weak dependence power.

The result of the MICMAC analysis for QS transition is shown in the driving and dependence power diagram in **Figure 1**.

4.2 Driving and Dependence Power Diagram for QS Transition

After obtaining the driving power and dependence power of each QS transition challenge, the challenge is placed in one of the four quadrants in the power diagram (autonomous, dependent, linkage, and independent). **Figure 1** shows the categorization of QS transition challenges in four quadrants based on the MICMAC approach, and the results are discussed below.

Autonomous: A set of challenges in this quadrant has weak driving power and weak dependence power, which signals that the challenges are relatively disconnected from the context. For the QS transition, no transition challenges were placed in an autonomous quadrant. Having no challenge belonging to the autonomous set indicates that all 15 QS transition challenges have a significant influence on the QS transition.

Dependent: A set of challenges in this quadrant has weak driving power and strong dependence power. The challenges with strong dependence power would require all other QS transition challenges to address the QS transition. For the QS transition, no transition challenges were placed in a dependent quadrant. This indicates that no QS transition challenges have weak driving power and strong dependence power.

Linkage: A set of challenges in this quadrant has strong driving power and strong dependence power. Having both strong driving power and dependence power signals that addressing change regarding the challenge will impact other challenges and have impact on themselves. For the QS transition, all 15 QS transition challenges were placed in the linkage quadrant. This indicates that all the QS transition challenges are interrelated and they impact each other.

Independent: A set of challenges in this quadrant has strong driving power and weak dependence power. These factors are also known as key factors falling into the quadrant of independent or linkage. The challenges with strong driving power can impact other challenges, which should be given priority. For QS transition, no transition challenges were placed in an independent quadrant and this indicates that key factors for QS may still need to be identified.

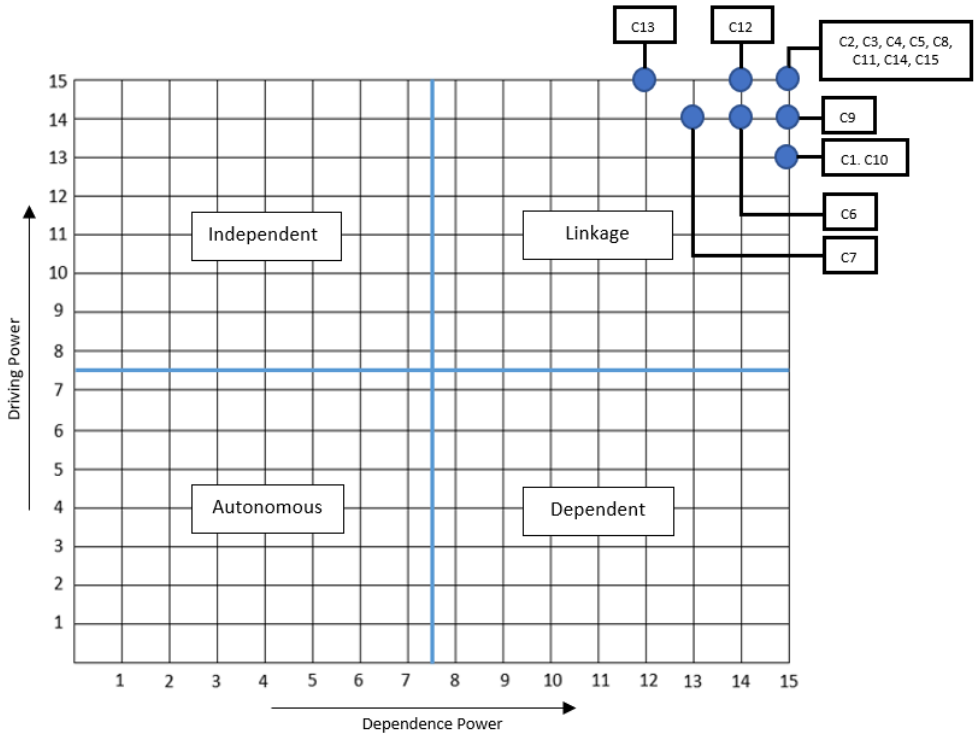

Figure 1. *Driving Power and Dependence Power Diagram*

4.3 ISM-based Hierarchy for QS Transition

The result of ISM-based hierarchy for QS transition shows that there are four levels of hierarchy. While the top level (Level 1) consists of challenges that have weak driving power, the lower level of the hierarchy consists of challenges that have stronger driving power. Thus, challenges in the lowest level (Level 4) have the strongest driving power among the QS transition challenges. ***Figure 2*** shows the ISM-based hierarchical model of QS transition challenges.

In Level 4, there are two challenges which include: Unclear QS Governance in the Ecosystem (C12) and a Lack of Collaboration in the Ecosystem (C13). In Level 3, there are eight challenges which include: No Availability of QS Standardization (C2), No QS Standards & Selection (C3), No Reliable & Secure QS Solutions (C4), No Availability of QS Hardware & Software (C5), No Business Case for

Organizations (C8), Lack of Urgency in the Ecosystem (C11), Lack of Policy & Regulations for QS Solutions (C14) and Complex Technological Interdependency in the Ecosystem (C15). In Level 2, there are three challenges which include: Knowledge Needs within Organizations (C6), Lack of Urgency within Organizations (C7), and Lack of Technical Skills & Qualified Personnel (C9). In Level 1, there are two challenges which include: Legacy System Constraints (C1) and Unclear QS Governance within Organizations (C10).

The result of QS transition challenges in the ISM-based hierarchy concludes that two challenges in the organizational context such as Legacy System Constraints (C1) and Unclear QS Governance within Organizations (C10) have the weak driving power and are influenced a whole range of other challenges in the lower hierarchy (Level 2-4). At first glance, making changes in the legacy systems and establishing the QS governance within organizations do not seem complex due to the scope of change being within organizations. However, the results show that addressing the QS transition within organizations is much more complicated. Since QS transition challenges are interdependent, challenges that exist at the lower hierarchy may first need to be addressed before the challenges at the top hierarchy are addressed.

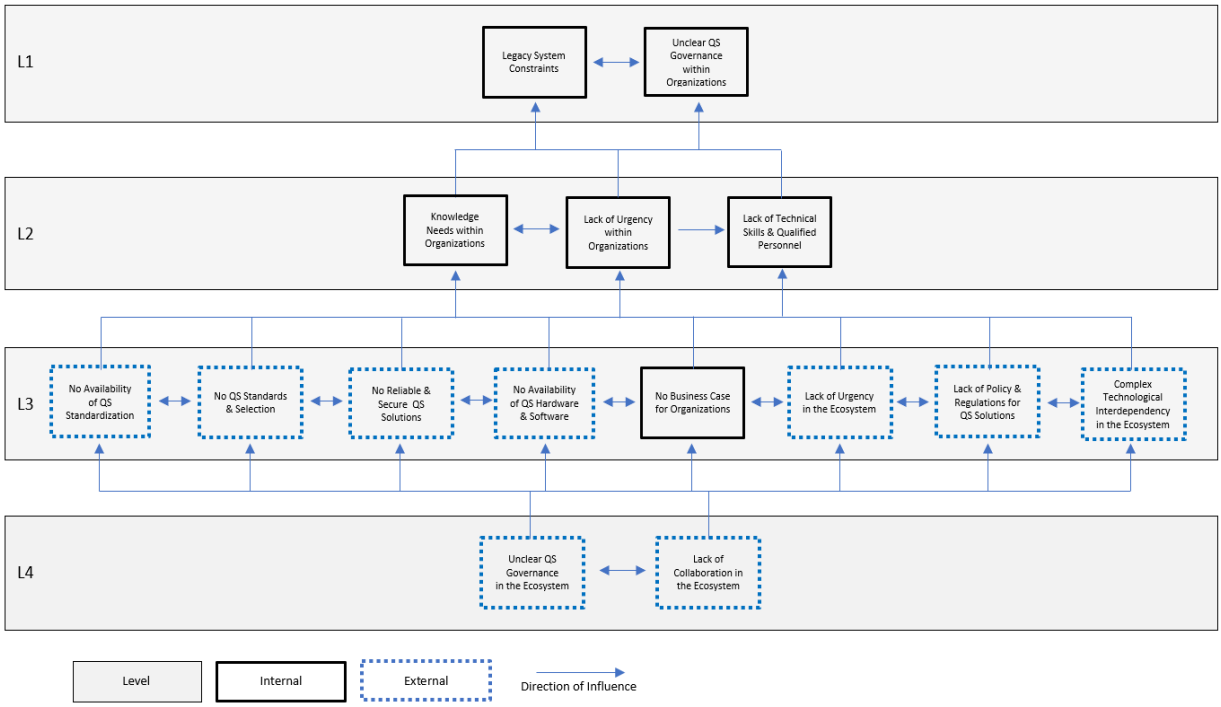

Figure 2. *ISM-based Hierarchy for QS Transition*

5 Discussion

This section provides discussions on data analysis and results of the ISM-MICMAC approach. The Driving and Dependence Power Diagram in ***Figure 1*** shows that all QS transition challenges were placed in the linkage quadrant. While QS transition challenges are interrelated, it also indicates that the QS transition is complex and not stable in nature. If there is a delay in one challenge, it can result in delays in other challenges. This implies that the QS transition is still at an early stage, and organizations may need to navigate the transition through a constantly changing environment. Also, there is a non-occurrence of autonomous, dependent, and independent challenges. While this indicates that the list of challenges used in the workshop is all relevant to the topic of QS transition, having no independent challenges with strong driving power and weak dependence power also signals that there is no single challenge that can act as a key factor for the QS transition.

Moreover, the ISM-based hierarchy in ***Figure 2*** provides an overview of QS transition challenges. Since establishing QS governance and collaboration in the ecosystem have the highest driving power among the QS transition challenges, addressing these challenges can influence other challenges in the

higher hierarchy (e.g. Levels 1-3). This highlights that the QS transition cannot be single-handled by one organization and require multiple actors in the PKI ecosystem to be part of the transition. However, there is a clear institutional void for the QS transition, and many actors in the decentralized nature of Dutch government PKIs require well-defined roles and responsibilities for the QS transition. Thus, achieving *collective action* in the PKI ecosystem is viewed as a priority, and establishing QS governance. There are various actors in the PKI ecosystem, and public sector is viewed very decentralized. Thus, addressing collaboration may further crystalize uncertainties in both technological and ecosystem context.

In addition, there are many challenges positioned in Level 3, and these include challenges that require external decisions. While four of these challenges are from the technological context (e.g. QS standardization, QS standards & selection, secure QS solutions, and QS hardware & software), the other three challenges are from the ecosystem context (e.g. urgency, policy & regulations for QS solutions and complex technological interdependencies). Only one challenge belongs to an organizational context (e.g. having QS transition business cases). This indicates that an external influence is needed across ministries to proceed with the transition and having business case in organizations may need to align with the PKI ecosystem they are in. Also, multiple challenges may need to be addressed synchronously in this level. If everyone is just waiting for each other, delays in one challenge can eventually create a *Catch-22* loop scenario which may lead to a deadlock for the QS transition.

Furthermore, the challenges in Level 2 and Level 1 relate to the organizational context. Having urgency within organizations can address knowledge needs and getting technical skills & qualified personnel within organizations. Although the organizations require external pressures from the lower hierarchy (e.g. Level 3-4), if organizations already know their cryptographic assets and the impact of quantum threats in their inventories, it may be possible to raise the level of urgency within organizations. In Level 1, establishing QS governance within organizations and making changes to legacy system constraints will only be addressed once many of the technological uncertainties are discussed and decisions are made in the PKI ecosystem. This also highlights that multiple actors in the PKI ecosystem may be involved in the different timelines of the QS transition. While some actors may be involved in making external decisions in the ecosystem, other actors may wait for those decisions and follow the lead.

6 Conclusion

The PKI not only provides digital communication and information sharing but also supports the security of other critical infrastructures across the national government. With ever-increasing dependency on PKIs and the possible obsolescence of such infrastructure against quantum threats raises the need to become quantum-safe. This paper takes a closer look at the QS transition challenges in governmental PKIs and provides more in-depth understanding of QS transition. While this paper is the first to present the views of QS transition across governmental PKIs, it is also the first to use a systemic approach to examine the contextual relationship between QS transition challenges.

The findings of the paper suggest that QS transition challenges in the ecosystem context and technological context must be addressed synchronously. Surprisingly, the analyses show that all the QS transition challenges are interrelated and will impact each other. Nonetheless, QS transition for the government PKIs cannot be addressed by a single organization and requires decisions to be discussed across ministries. By prioritizing the QS governance and collaboration in the ecosystem, other important actors in the ecosystem may be included, and it would set the scene for discussions that is necessary for the QS transition. While the nature of the QS transition challenges is volatile, if uncertainties surrounding the technological context and ecosystem context are not addressed in time, it would be much more challenging for organizations to navigate the transition.

Although the results of ISM-based hierarchy and MICMAC analysis provide a directional structure for the QS transition, the analysis also shows that it is a complex problem in which QS transition challenges are heavily related to one another and actors in the governmental PKIs are interdependent. While the results indicate that the QS transition is still at its early stage, it shows that there is no single solution that can address the QS transition, and it is crucial to address both socio-technical predicaments. Going forth, since legacy system constraints and QS governance within organizations

can be influenced by challenges in the lower hierarchy (Level 2-4), other actions may be needed for organizations that are looking to become frontrunners for the QS transition.

Moreover, the paper also found that there are still many more QS transition research opportunities left to be conducted. While this paper provides the starting point to understand the QS transition and the dynamics between QS transition challenges, it would also be important to validate the findings with other experts in the PKI ecosystem to understand different perspectives of QS transition challenges. Perhaps, the workshops can also be conducted with different actors in different PKI ecosystems other than governmental PKIs to understand the directions that organizations need to prioritize. Furthermore, it would be worthwhile to identify what needs to be included in the discussion among different actors in the PKI ecosystem and further examine some in-between steps that are considered important in addressing the QS transition challenges.

7 Acknowledgements

This publication is part of the HAPKIDO research project with project number NWA.1215.18.002 of the research programme Cybersecurity, which is (partly) financed by the Dutch Research Council (NWO).

8 References

1. Broeders, D., *The Secret in the Information Society.* Philosophy & Technology, 2016. **29**(3): p. 293-305.
2. Quach, S., et al., *Digital technologies: tensions in privacy and data.* J Acad Mark Sci, 2022. **50**(6): p. 1299-1323.
3. Haber, E. and T. Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis.* Florida State University Law Review, 2017. **44**(2).
4. Tikk, E., *Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective.* 2018.
5. Grover, L.K., *A fast quantum mechanical algorithm for database search.* 1996.
6. Shor, P.W., *Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer*. 1994.
7. Barker, W., W. Polk, and M. Souppaya, *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*. 2021.
8. Mavroeidis, V., et al., *The Impact of Quantum Computing on Present Cryptography.* International Journal of Advanced Computer Science and Applications (IJACSA), 2018. **9**(3).
9. Yunakovsky, S.E., et al., *Towards security recommendations for public-key infrastructures for production environments in the post-quantum era.* EPJ Quantum Technology, 2021. **8**(1).
10. NIST, *Report on Post-Quantum Cryptography*, L. Chen, et al., Editors. 2016, National Institute of Standards and Technology, U.S. Department of Commerce.
11. NIST. *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates.* 2022; Available from: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.
12. Barker, W., M. Souppaya, and W. Newhouse, *Migration to Post-Quantum Cryptography*. 2021.
13. Bindel, N., et al., *Transitioning to a Quantum-Resistant Public Key Infrastructure.* 2017.
14. CCC, *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*. 2019, Computing Community Consortium.
15. Kong, I., M. Janssen, and N. Bharosa, *Challenges in the Transition towards a Quantum-safe Government*, in *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*. 2022. p. 282-292.
16. McKinseyDigital., *When—and how—to prepare for post-quantum cryptography*. 2022.
17. Tibbetts, J., *Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decision Makers*. 2019, UC Berkeley: Center for Global Security Research.

18. TNO, *Migration to Quantum-safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-safe situation* F. Muller and M.P.P. van Heesch, Editors. 2020.
19. TNO, CWI, and AIVD, *The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography*. 2023.
20. Vermeer, M.J.D. and E.D. Peet, *Securing Communications in the Quantum Communications in the Quantum Computing Age: Managing the Risks to Encryption* 2020, RAND Corporation.
21. Bharosa, N., et al., *Challenging the Chain - Governing the Automated Exchange and Processing of Business Information*. 2015.
22. Hunt, R., *Technological infrastructure for PKI and digital certification.* Computer Communications, 2001. **24**: p. 1460-1471.
23. Linn, J., *Trust Models and Management in Public-Key Infrastructures.* 2000.
24. Adner, R., *Ecosystem as Structure.* Journal of Management, 2017. **43**(1): p. 39-58.
25. Innovalor, *PKIoverheid: Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling.* . 2019.
26. SSC-ICT. *Jaarverslag SSC-ICT 2018*. 2018; Available from: https://www.ssc-ictspecials.nl/jaarverslag-ssc-ict/2018/01.
27. Logius, *CERTIFICATION PRACTICE STATEMENT (CPS): Policy Authority PKIoverheid for Private Root CA certificates to be issued by the Policy Authority of the PKI for the Dutch government.* 2020.
28. Logius, *PKIoverheid Programme of Requirements v4.10: Part 3 Basic Requirements*. 2022, Ministrie van Binnenlandse Zaken en Koninkrijksrelaties.
29. NCSC, *PKIoverheid is changing*. 2020, National Cyber Security Center, Ministry of Justice and Security.
30. CSIRO, *The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography*. 2021.
31. Huang, J. and D.M. Nicol, *An anatomy of trust in public key infrastructure.* International Journal of Critical Infrastructures, 2017. **13(**2/3).
32. Baker, J., *The Technology–Organization–Environment Framework*, in *Information Systems Theory*. 2011. p. 231-245.
33. Tornatzky, L.G., M. Fleischer, and A.K. Chakrabarti, *Processes of Technological Innovation. Lexington Books, Lexington.* 1990: Lexington Books, Lexington.
34. Warfield, J.N., *Toward Interpretation of Complex Structural Models.* IEEE Transactions on Systems, Man, and Cybernetics, 1974. **SMC-4**(5): p. 405-417.
35. Janssen, M., et al., *Challenges for adopting and implementing IoT in smart cities.* Internet Research, 2019. **29**(6): p. 1589-1616.
36. Usmani, M.S., et al., *Identification and ranking of enablers to green technology adoption for manufacturing firms using an ISM-MICMAC approach.* Environ Sci Pollut Res Int, 2023.
37. Godet, M. *Methods of Prospective*. 1971; Available from: http://en.laprospective.fr/methods-of-prospective/softwares---cloud-version/4-micmac.html.
38. Attri, R., N. Dev, and V. Sharma, *Interpretive Structural Modelling (ISM) approach: An Overview.* Research Journal of Management Sciences, 2013. **2**(2).
39. Deepu, T.S. and V. Ravi, *An ISM-MICMAC approach for analyzing dependencies among barriers of supply chain digitalization.* Journal of Modelling in Management, 2022.

Appendix 1. List of QS Transition Challenges

Technological Challenges	Code	Description
Legacy System Constraints	C1	The existing system is rigid and only supports a handful of algorithms. The existing system may need changes in the hardware and/ or software depending on the compatibility of new QS solutions.
No Availability of QS Standardization	C2	NIST is currently selecting practical standards and guidelines for QS solutions. Thus, stardards for QS cryptographic algorithms are not yet available.
No QS Standards & Selection	C3	Organization has not yet selected which QS solutions will be used and whether or not to have a full substitution of QS solution or a hybrid solution. The selection criteria for QS solutions are not clear. Trade-offs in the performance outcomes and usage context of QS solutions may need to be examined.
No Reliable & Secure QS Solutions	C4	The QS solutions have not been tested and currently, there is no testing is available to prove the security of QS solutions.
No Availability of Certified QS Hardware & Software	C5	The suppliers of the current technology are not yet ready to provide the certified technology compartments for the replacement technology. e.g. HSM and certificate issuance software for QS solutions.
Organizational Challenges	**Code**	**Description**
Knowledge Needs within Organizations	C6	There is a lack of knowledge on quantum computing-based threats, and risks associated with the technology in organizational assets e.g. cryptographic assets, and vulnerabilities etc.
Lack of Urgency within Organizations	C7	The arrival of a large-scale quantum computer is perceived to be decades away, and there is a lack of urgency for QS transition in organizations.
No Business Case for Organizations	C8	Organization finds it difficult to enter long-term QS transition commitments without clear business benefits and opportunities.
Lack of Technical Skills & Qualified Personnel	C9	There is a lack of qualified personnel who can understand QS solutions and make decisions on the implementation process.
Unclear QS Governance within Organizations	C10	Organization does not have transition plans and they do not know what to prioritize for QS transition.
Ecosystem Challenges	**Code**	**Description**
Lack of Urgency in the Ecosystem	C11	There is a lack of collective sense of urgency and it is difficult to achieve inter-agency coordination and collaborations with multiple stakeholders.
Unclear QS Governance in the Ecosystem	C12	Organization does not know which organizations are in the lead and who takes responsibility for what.
Lack of Collaboration in the Ecosystem	C13	The varying levels of interests, needs and expectations contribute to duplication of efforts, limited knowledge sharing and fragmented decision making within the ecosystem.
Lack of Policy & Regulations for QS Solutions	C14	There is a lack of policy and legal implications for the QS transition, and compliances for QS solutions need to be updated.
Complex Technological Interdependency in the Ecosystem	C15	Changes in the existing system cannot occur in isolation due to its chain of interdependencies including governing bodies, standards bodies, hardware providers, third-party software providers etc. e.g. A software developer that creates software using new QS standards is needed for end users, and impact on end users is just as important as the impact on Trust Service Providers etc.