TU Delft

Delft University of Technology

Transitioning Towards Quantum-Safe Government

Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems

Kong, Ini

DOI
10.1145/3560107.3560182

Publication date
2022

Document Version
Final published version

Published in
Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022

Citation (APA)
Kong, I. (2022). Transitioning Towards Quantum-Safe Government: Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems. In L. Amaral, D. Soares, & L. Zheng (Eds.), *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022* (pp. 499-503). (ACM International Conference Proceeding Series). Association for Computing Machinery (ACM). https://doi.org/10.1145/3560107.3560182

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Transitioning Towards Quantum-Safe Government

Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems

Ini, Kong*
Faculty of Technology, Policy, and Management, Delft University of Technology
i.kong@tudelft.nl

ABSTRACT

Public Key Infrastructures (PKIs) provide digital public services and communication by securing information-sharing and strong credentials for digital identity management to individuals, businesses, and government agencies. While cryptographic algorithms that current PKI systems depend on are mostly resilient against hacks and other threats launched from computers we use today, the advancement of quantum computing technology introduces new security threats. This calls for current PKI systems to be modified with quantum-safe cryptographic algorithms. However, transitioning to Quantum-safe (QS) PKI systems remains complex, and the challenges are socio-technical. The research aims to guide organizations transitioning towards QS PKI systems. In doing so, we will deconstruct the QS transition into a series of stages and paths using growth models and examine how organizations can transit over time towards QS PKI systems.

KEYWORDS

Quantum-Safe Transition, Public Key Infrastructure, Stages of Growth Models, Quantum-Safe Government

ACM Reference Format:
Ini, Kong. 2022. Transitioning Towards Quantum-Safe Government: Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems. In *15th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2022), October 04–07, 2022, Guimarães, Portugal.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3560107.3560182

1 INTRODUCTION

At the core of Europe's electronic identification scheme and communication infrastructures, Public Key Infrastructures (PKIs) provide digital communication and secure information exchange [1., 2.]. PKIs enable communications between citizens/clients, public agencies, web applications, data centers and inter-governmental organizations [3., 4.]. Without requiring the physical presence of users, PKIs generate, store, distribute and manage digital certificates used in digital transactions [5., 6.]. The cryptographic algorithms that digital certificates in the PKI systems depend on are demonstrated to be mostly resilient against hacks and other threats launched from computers we use today [7.].

*Corresponding author

This work is licensed under a Creative Commons Attribution International 4.0 License.

ICEGOV 2022, October 04–07, 2022, Guimarães, Portugal
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9635-6/22/10.
https://doi.org/10.1145/3560107.3560182

However, the computation power of quantum computing introduces new security threats. On the one hand, quantum computers have the potential to perform computations much more quickly than classical computers and break widely-used key encryption schemes (eg. using Shor's algorithm and Grover's algorithm), including the cryptographic algorithms that PKI depends on [8., 9.]. On the other hand, *store now-decrypt later* can occur without having a large-scale quantum computer [10.]. The information that requires long-term security can be harvested, stored now, and decrypted later once the quantum computers become available [11., 12.].

In order to mitigate against quantum-computing-based threats, current PKI systems need to modify cryptographic algorithms to the one that is quantum-safe (QS) [11., 13.-16.]. Recently, NIST has identified four candidate algorithms for standardization (eg. **CRYSTALS-KYBER for public key encryption and CRYSTALS-Dilithium, FALCON,** and **SPHINCS$^+$** for digital signatures) [17.]. However, the development of QS cryptographic standards are ongoing and the debate on which QS cryptographic standards are suitable for PKI systems remain undecided [18.-21.].

Moreover, transitioning to QS PKI systems require collaboration on many levels. There are multiple stakeholders, including governments, standards bodies, hardware vendors, software companies, service providers, and PKI users [20.]. The varying levels of urgency, interest, and expectation make it difficult to coordinate the transition process [22.-24.]. The organizations need to draw up transition plans and recognize the amount of lead-time required for the QS transition. However, there is a void in knowledge as organizations are unprepared and do not know where to begin the QS transition [11., 14., 19., 25.]

Our research aims to guide organizations transitioning towards QS PKI systems. In doing so, we deconstruct the QS transition into a series of stages and paths using growth models and examine how organizations can transit over time towards QS PKI systems [26., 27.]. In each stage, we identify capabilities needed in the current PKI systems and how organizations can evolve over time toward QS PKI systems [28., 29.].

The following research questions have been formulated to achieve the research aim. The main research question is:

> "How can organizations transit towards Quantum-safe (QS) PKI systems?"

To answer the main research question, there are several sub-questions that have been formulated.

- RQ1.What are the challenges that hinder organizations in transitioning toward QS PKI systems?
- RQ2. What are the different stages needed in growth models for QS PKI systems?
- RQ2a. What capabilities per stage are needed in transitioning to QS PKI systems?

- RQ2b. What are the requirements and constraints of growth models for QS PKI systems?
- RQ3. Which transition paths follow from the growth model self-evaluation?

2 PROBLEM ANALYSIS

This section presents an overview of the research problem to our topic of research.

2.1 Quantum-safe (QS) Transition

2.1.1 Threats to the current PKI system. The current PKI systems depend on the public key cryptography that is based on complex mathematical problems. The public key cryptography, also known as asymmetric cryptography, uses a key pair, including one public key that must be verifiably authentic and one private key that must remain private [4., 5.]. These keys are mathematically tied together, so the private key can only decrypt the encrypted information using its corresponding public key [12.]. The modern public key cryptography seem to be mostly resilient against hacks and other threats launched from computers we use today.

However, it is no longer safeguarded against the quantum-computing-based threats for two reasons. Firstly, quantum computers can perform computations much more quickly than classical computers. Using Shor's algorithm, quantum computers can bypass time-consuming process and enable a key extraction of the private key [8.]. For those cryptographic algorithms that are not affected by Shor's algorithm, Grover's algorithm offers a shortcut and allows quantum computers to speed up the search process of keys [9.]

Secondly, *store now-decrypt later* can occur even today without having a large-scale quantum computer [10.]. Any data that needs to remain secure for the next 10-20 years are at risk [16.]. This is because unauthorized parties can harvest the data, store it now in an encrypted form and be able to decrypt it in the future once a quantum computer becomes available [10.]. Since organizations often do not know whether the information has already been harvested and stored, it is crucial that sensitive data are protected to prevent possible future attacks [10., 30.]

2.1.2 Quantum-Safe (QS) Cryptography. The two main areas for quantum-safe cryptography include (a) Post Quantum Cryptography (PQC) and (b) Quantum Key Distribution (QKD). While PQC is based on asymmetric encryption methods and may work across the existing PKI infrastructure, QKD is a hardware-based approach that uses the properties of quantum physics called quantum bits (qubits) [31.]. These quantum properties include 1. *Superposition* that can represent 0 and 1 simultaneously, and 2. *Entanglement* where the state of one entangled particle can change the state of all other entangled particles [10., 32.].

Although both solution directions hold appealing properties that are promising, different limitations exist in terms of optimization and performance [11.]. Recently, the National Institute of Standards and Technology (NIST) has identified four candidate algorithms for standardization. (eg. **CRYSTALS-KYBER for public key encryption, and CRYSTALS-Dilithium, FALCON**, and **SPHINCS$^+$** for digital signatures) [17.]. Further research is taking place in order to identify many distributed computing scenarios, usage contexts, and hardware-based security schemes to better substitute existing algorithms [33.-35.].

According to Mosca (2015), the transition from the current PKI systems need to be planned as soon as possible to prevent potential risks [16.]. However, whether organizations require the full substitution of *quantum-safe* (QS) cryptographic algorithms or hybrid solution (that includes both classical and QS algorithms) are not yet decided. The organizations often do not know their vulnerabilities and it is difficult to assess where and what needs to be prioritized for the QS transition [11., 33., 36., 37.]

3 THEORETICAL LENS

This section presents an overview of the theoretical lens to our topic of research.

3.1 Stages of Growth Models

The concept of stages of growth models has become an important topic in both IS research and practice. The examples of growth models have their landmark reference to Nolan's Stage of Growth Theory (1973). It is also referred to as *stages of growth* or *stage models* [38.-40.]. The stages of the growth model develop an understanding of the evolution of information technology and how technologies have evolved and continue to evolve in organizations [28., 29.]. In each stage of the growth model, new tasks and problems need to be addressed in order to move from one stage to the next [27.]. The concept of discontinuity is used as a demarcation between stages where different capabilities may need to reach the next stages [41., 42.]. By identifying and assessing capabilities in each stage, the stage in organizations can provide guidelines for future improvements [27., 43.].

Despite the extensive development of growth models in IS field, the stages of the growth models do not have a systematic approach in deriving at different stages of the model. While some growth models are exception to this criticism (eg. [42.], [41.], [44.], [45.]), the majority of models do not have theoretical or empirical foundations and remain largely conceptual. The oversimplification of the model shows a little variation towards maturity and the process is much more complex in practice [46., 47.]. Moreover, the growth models do not act as silver bullets as they are designed to meet desired objectives which may differ from one context to another. However, currently there is no ready-to-use growth model in the context of QS transition. Organizations can identify the stage they are positioned and challenges that need to be addressed to achieve QS PKI systems. This would provide a better understanding on QS transition paths that are currently unclear for organizations [48., 49.].

3.2 Organizational Capabilities

With organizational assets such as people, knowledge and capabilities, the creation and refinement of capabilities allow organizations to achieve better outcomes or performance, adapt and organize themselves [41.]. As stages of growth model provide a roadmap for organization to achieve its desired stage from moving one stage to the next, the concept of capabilities at an organizational level enriches details on internal dynamics of organization's growth. In order to understand how organization transforms to the desired

level (to-be situation) in distinct stages, the concept of capabilities seem to be complementary to organizational growth. In order to understand how organization transforms to the desired level (to-be situation) in distinct stages, the concept of capabilities seem to be complementary to organizational growth.

The concept of organizational capabilities show that capabilities is crucial not only for organizations to reinvent and go through a transformation but also to reintroduce operational activities that meet the changing environment [50.-52.]. The modification and reconfiguration of existing intangible or tangible assets of organizations can further create new strategic assets (such as technology, collaboration, capability and complementary assets) [51., 53.-55.]. The work of [51.] and [56.] distinguish that traditional capabilities focus on doing things right, and dynamic capabilities focus on doing the right things which finds opportunities and facilitates innovation [51., 56.]. The work of [50.] defines ordinary capabilities to enable organizational performance, and dynamic capabilities to invoke the changes to ensure ordinary capabilities perform [50.].

Although much of the research on capabilities are divided into two approaches either as the ability-based approach [51., 55.-57.] or the routine-based approach [50., 52., 58.], there is a lack of agreement in the definitions and components regarding the term. This provides an opportunity to consider diverse definitions and further extend the term in the context of the study. Moreover, there is no generic list of organizational capabilities that can be applied to all types of activities and settings. In the context of QS transition, there is no set of established capabilities that can provide guidelines for practitioners in order to develop capabilities and reconfigure resources. This results in unclear practical implications for capabilities needed for QS transition.

4 METHODOLOGY

This section provides research strategies and proposed research methods.

4.1 Case Study Research

In the context of our research, the topic on QS PKI transition is relatively new and there is a lack of ready-to-use growth model available for QS transition. Likewise, existing theories are inadequate and there is no systematic approach for deriving different stage of the growth models. Since the case study research aims to develop a novel, accurate, and robust theory that emerges from the collected data, it can address theoretical gaps when existing theories are inadequate in solving the problem of the research context [59., 60.].

Moreover, we address the "what" and "how" types of questions using multiple case studies with multiple embedded units of analysis. Multiple case studies offer comparative perspectives and are advantageous when identifying theoretically relevant constructs with strong empirical basis [59.]. In addition, the research examines Dutch PKI systems in governments which include multiple units of analysis with various organizations that are involved. Having more than one unit of analysis strengthens the empirical investigation of a phenomenon from multiple sources of evidence [59., 60.].

In order to sufficiently gather different perspectives of the PKI systems, theoretical sampling is used to select multiple units of analysis in the study selection. For the purpose of theoretical sampling, the units of analysis in the study are part of the PKI systems in governments. The multiple organizations include users of PKI systems (eg. Tax authority, Chamber of Commerce, banks), organizations that govern PKI systems (eg. Logius, Ministry of Internal Affairs), and organizations that provide external expertise (eg. Qualified Trust Service Providers). Since various organizations in the PKI systems are involved, the growth models are developed for these organizations.

4.2 Proposed Research Methods

4.2.1 Phase 1: Systematic Literature Review, Expert Interview. RQ1. What are the challenges that hinder organizations in transitioning toward QS PKI systems?

Research question 1 intends to construct a knowledge base for the PKI systems. We divide this phase into two different parts. First, we conduct a Systematic Literature Review (SLR) to identify relevant challenges that organizations may encounter when transitioning toward QS PKI systems. Second, we conduct expert interviews with organizations that are part of the PKI systems to understand the challenges in practice.

4.2.2 Phase 2: ISM-MICMAC, Systematic Literature Review, Expert Interviews. RQ2a. What capabilities per stage are needed in transitioning to QS PKI systems?

Research question 2a intends to examine capabilities that are needed to address the challenges found in Phase 1. We use the Interpretive Structural Modelling & Cross-Impact Matrix Multiplication (ISM-MICMAC) approach. Moreover, we will conduct another SLR as a starting point to identify the list of capabilities in literature. Then, we will conduct expert interviews to refine the list of capabilities available and needed in organizations.

4.2.3 Phase 3 Expert Interview, Workshops, Synthesis. RQ2b. What are the requirements and constraints in transitioning to QS PKI systems?

Research question 2b intends to position different capabilities in growth models. We will conduct another set of expert interviews to identify the requirements and constraints of growth models. Moreover, the results from Phase 2 will further be used as an input to provide an overview of capabilities for the stages of the growth models. The results from the literature, expert interviews, and workshops will be synthesized.

4.2.4 Phase 4 Workshop & Survey. RQ3. Which transition paths follow from the growth model self-evaluation?

Research question 3 intends to evaluate growth models by collecting feedback from organizations. We conduct a series of workshops: 1. To check whether all the requirements for the growth model have been included 2. To assess the growth models using criteria (eg. quality, content, and utility). Furthermore, an online self-assessment tool will be created to collect additional data from organizations that are part of PKI systems in government.

5 PRELIMINARY RESULTS AND RESEARCH CONTRIBUTION

This section presents an overview of DG.O 2022 conference paper and research contribution.

5.1 Digital Government Society Conference Paper

The first part of Phase 1 described in Section 4.2.1 has been conducted, and the paper has been published in the 23rd Annual International Conference on Digital Government Research (DG.O 2022) [61.]. The results gathered from the literature build knowledge on relevant challenges that organizations may encounter when transitioning towards a QS PKI system. The challenges were further clustered using Technology-Organization-Environment (TOE) framework. The main challenges in the technological context include no universal QS solution, legacy system, complex PKI interoperability, and vulnerable Root CA. The main challenges in the organizational context include knowledge gap, unclear governance, lack of urgency, and in-house management support. Furthermore, the main challenges in the environmental context include institutional void, stakeholder collaboration, lack of awareness, and policy guidance. The results indicate that the QS transition from the current PKI system is complex, and the challenges are socio-technical [61.].

5.2 Research Contribution

The research has a scientific contribution as it provides a new body of knowledge in the field of Information Systems and Digital Government. First, The QS cryptographic algorithm is a new technology, and there is a gap in the literature on how to transition toward QS PKI systems. The research further enriches the knowledge in organizational management and development of QS PKI systems in government. Second, the research identifies how organizations can derive different stages of growth models for QS transition and extends theoretical linkages on growth models.

Next to the scientific contribution, the research has a societal contribution. First, the study is a part of a larger research project called HAPKIDO (Hybrid Approach for quantum-safe Public Key Infrastructure Development for Organizations), which is funded by NOW (Netherlands Organization for Scientific Research). The organizations can benefit from the study output once it becomes publically available. Second, the QS transition can be deconstructed and understood in a series of different stages. By identifying the capabilities needed for QS transition in each stage, organizations can prepare and provide an operational approach toward QS PKI systems.

ACKNOWLEDGMENTS

This paper is part of my dissertation proposal and 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).

REFERENCES

[1.] ENISA, *Post-Quantum Cryptography: Current state and quantum mitigation*. 2021, European Union Agency for Cyber Security.
[2.] EuropeanCommission, *EU Security Union Strategy*. 2020.
[3.] Burr, W.E. and K.L. Lyons-Burke, *Public Key Infrastructures for the Financial Services Industry*. 1999.
[4.] Hunt, R., *Technological Infrastructure for PKI and Digital Certification*. Computer Communications, 2001. **24**: p. 1460-1471.
[5.] Adams, C. and S. Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*. 1999: Macmillan Technical Publishing.
[6.] Linn, J., Trust Models and Management in Public-Key Infrastructures. 2000.
[7.] Bharosa, N., *et al.*, Challegning the Chain: Governing the automated exchange and processing of business information. 2015: Logius & Thauris.
[8.] Shor, P.W., Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer. 1994.
[9.] Grover, L.K., *A fast quantum mechanical algorithm for database search*. 1996.
[10.] Mavroeidis, V., *et al.*, *The Impact of Quantum Computing on Present Cryptography*. International Journal of Advanced Computer Science and Applications,, 2018.
[11.] NIST, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms. 2021.
[12.] 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).
[13.] de Wolf, R., *The potential impact of quantum computers on society*. Ethics and Information Technology, 2017. **19**(4): p. 271-276.
[14.] Mulholland, J., M. Mosca, and J. Braun, *The Day the Cryptography Dies*. IEEE Security & Privacy, 2017: p. 14-21.
[15.] NIST, *Report on Post-Quantum Cryptography*, L. Chen, *et al.*, Editors. 2016.
[16.] Mosca, M., Cybersecurity in an era with quantum computers: will we be ready? 2015.
[17.] NIST. *PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates*. 2022 [cited 2022 08-08]; Available from: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.
[18.] ISARA, Enabling Quantum-Safe Migration with Crypto-Agile Certificates. 2018.
[19.] Machatan, A. and D. Heintzman, *The Complex Path to Quantum Resistance*. 2021.
[20.] CCC, Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. 2019, Computing Community Consortium
[21.] Bindel, N., *et al.*, *Transitioning to a Quantum-Resistant Public Key Infrastructure*. 2017.
[22.] Vermeer, M.J.D. and E.D. Peet, Securing Communications in the Quantum Computing Age: Making the risks to encryption. 2020.
[23.] Chen, L. and D. Moody, *New mission and opportunity for mathematics researchers: cryptography in the quantum era*. Advances in Mathematics of Communications, 2020. **14**(1): p. 161-169.
[24.] Räsänen, M., *et al.*, *Path to European quantum unicorns*. EPJ Quantum Technol, 2021. **8**(1): p. 5.
[25.] Vermaas, P.E., *The Societal Impact of the Emerging Quantum Technologies: A Renewed Urgency to Make Quantum Theory Understandable*. Ethics and Information Technology, 2017. **19**(4): p. 241-246.
[26.] Teo, T.S.H. and W.R. King, *Integration between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective*. Journal of Management Information Systems, 1997. **14**(1): p. 185-214.
[27.] Kazanjian, R.K. and R. Drazin, *An Empirical Test of a Stage of Growth Progression Model*. Management Science, 1989. **35**(12): p. 1489-1503.
[28.] Gibson, C. and R. Nolan, *Managing the Four Stages of EDP Growth*. Harvard Business Review, 1974. **52**.
[29.] Nolan, R.L., *Managing the computer resource: a stage hypothesis*. Commun. ACM, 1973. **16**(7): p. 399–405.
[30.] NIST, The Economic Impacts of the Advanced Encryption standard, 1996–2017. 2018.
[31.] Hong, K.-W., O.-M. Foong, and T.-J. Low, Challenges in Quantum Key Distribution, in Proceedings of the 4th International Conference on Information and Network Security - ICINS '16. 2016. p. 29-33.
[32.] Gibney, E., *The Quantum Gold Rush*. 2019.
[33.] TheHagueSecurityDelta, Understanding the Strategic and Technical Significance of Technology for SecurityImplications of Quantum Computing within the Cybersecurity Domain Together. 2019.
[34.] Accenture, *In Quantum We Trust*. 2020.
[35.] Lovic, V., *Quantum Key Distribution: Advantages, Challenges and Policy*. Cambridge Journal of Science and Policy, 2020. **1**(2).
[36.] Grote, O., A. Ahrens, and C. Benavente-Peces, Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques, in Proceedings of the 9th International Conference on Pervasive and Embedded Computing and Communication Systems. 2019. p. 91-98.
[37.] Lindsay, J.R., *Surviving the Quantum Cryptocalypse*. 2020b.
[38.] Solli-Sæther, H. and P. Gottschalk, *The Modeling Process for Stage Models*. Journal of Organizational Computing and Electronic Commerce, 2010. **20**(3): p. 279-293.
[39.] Prananto, A., J. McKay, and P. Marshall, *A Study of the Progression of E-Business Maturity in Australian SMEs*. 2003.

[40.] Layne, K. and J. Lee, *Developing Fully Functional E-Government: A Four Stage Model*. Government Information Quarterly, 2001. **18**: p. 122-136.
[41.] Klievink, B. and M. Janssen, *Realizing joined-up government — Dynamic capabilities and stage models for transformation*. Government Information Quarterly, 2009. **26**(2): p. 275-284.
[42.] Janssen, M. and A.F. van Veenstra, *Stages of Growth in e-Government: An Architectural Approach*. The Electronic Journal of e-Government, 2005. **3**.
[43.] Gottschalk, P., *E-Government Interoperability*. IGI Global, 2009.
[44.] Lee, J., *10year retrospect on stage models of e-Government: A qualitative meta-synthesis*. Government Information Quarterly, 2010. **27**(3): p. 220-230.
[45.] Siau, K. and Y. Long, *Synthesizing E-Government Stage Models—A Meta-Synthesis Based on Meta-Ethnography Approach*. Industrial Management and Data Systems, 2005. **105**: p. 443-458.
[46.] de Bruin, T., *et al.*, *Understanding the Main Phases of Developing a Maturity Assessment Model*. Australasian Conference on Information Systems, 2005.
[47.] King, J.L. and K.L. Kraemer, *Evolution and organizational information systems: an assessment of Nolan's stage model*. Commun. ACM, 1984. **27**(5): p. 466–475.
[48.] Mehta, N., S. Oswald, and A. Mehta, *Infosys Technologies: improving organizational knowledge flows*. Journal of Information Technology, 2007. **22**: p. 456-464.
[49.] Rao, S., G. Metts, and C. Mora-Monge, *Electronic commerce development in small and medium sized enterprises: A stage model and its implications*. Business Process Management Journal, 2003. **9**: p. 11-32.
[50.] Eisenhardt, K.M. and J.A. Martin, *Dynamic Capabilities: What Are They?* Strategic Management Journal, 2000. **21**(10-11): p. 1105-1121.
[51.] Teece, D.J., *A dynamic capabilities-based entrepreneurial theory of multinational enterprise*. Journal of International Business Studies, 2014. **45**.
[52.] Winter, S.G., *Understanding dynamic capabilities*. Strategic Management Journal, 2003. **24**(10): p. 991-995.
[53.] Helfat, C., *et al.*, *Dynamic capabilities : understanding strategic change in organizations*. 2007, Malden, MA: Blackwell.
[54.] Helfat, C.E. and R. Winter, *Untangling dynamic and operational capabilities: strategy for the (n)ever-changing world*. Strategic Direction, 2011. **28**(3).
[55.] Teece, D.J., *Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance*. Strategic Management Journal, 2007. **28**(13): p. 1319-1350.
[56.] Teece, D.J., Dynamic capabilities and entrepreneurial management in large organizations: Toward a theory of the (entrepreneurial) firm. European Economic Review, 2016. **86**: p. 202-216.
[57.] Teece, D.J., G. Pisano, and A. Shuen, *Dynamic capabilities and strategic management*. Strategic Management Journal, 1997. **18**(7): p. 509–533.
[58.] Zollo, M. and S.G. Winter, *Deliberate Learning and the Evolution of Dynamic Capabilities*. Organization Science, 2002. **13**(3): p. 339-351.
[59.] Eisenhardt, K.M., *Building Theories from Case Study Research*. The Academy of Management Review, 1989. **14**(4): p. 520-550.
[60.] Eisenhardt, K.M. and M.E. Graebner, *Theory Building from Cases: Opportunities and Challenges*. The Academy of Management Journa, 2007. **50**(1): p. 25-32.
[61.] Kong, I., M. Janssen, and N. Bharosa, *Challenges in the transition towards a QS government*. 2022.