Deriving Government Roles for directing and supporting Quantum-safe Transitions

Ini, Kong; Marijn, Janssen; Nitesh, Bharosa

DOI
10.1145/3657054.3657114

Publication date
2024

Document Version
Final published version

Published in
Proceedings of the 25th Annual International Conference on Digital Government Research, DGO 2024

Deriving Government Roles for directing and supporting Quantum-safe Transitions

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

Marijn, Janssen
Faculty of Technology, Policy, and Management, Delft University of Technology
m.f.w.h.a.janssen@tudelft.nl

Nitesh, Bharosa
Faculty of Technology, Policy, and Management, Delft University of Technology
n.bharosa@tudelft.nl

ABSTRACT

Ensuring the secure provision of data and services using critical information infrastructures amidst the evolving technology landscape is a crucial yet recurrent task. However, these infrastructures can become vulnerable due to developments in quantum computing and modifying the infrastructures with quantum-safe (QS) technology is unlike regular control and maintenance. Organizations need to modify their cryptographic layers, which act as the fundamental building blocks of infrastructures. For organizations, many uncertainties pose challenges across technological, organizational and ecosystem areas. While QS technology is new and not yet available for implementation and adoption, changes in critical information infrastructures require collaboration among multiple public and private organizations spanning industries and borders. By understanding the roles, organizations may better understand what should be done for QS transitions. Until now, there has been no academic research examining the roles that government could or should play in QS transitions. This paper reveals 12 different roles, showing the diversity and breadth of actions needed. While there are many possible roles that still need to be allocated for coordinated efforts, there is a high reliance on the government, and organizations are waiting for and expecting governments to take more active roles in QS transitions. The results also signals that QS transition research is at its early stage with a clear governance void and lack of collective urgency in the ecosystem.

CCS CONCEPTS

• **General and reference** → Document types; General conference proceedings.

KEYWORDS

Quantum-safe, transition, information infrastructure, role, security, policy-making

ACM Reference Format:
Ini, Kong*, Marijn, Janssen, and Nitesh, Bharosa. 2024. Deriving Government Roles for directing and supporting Quantum-safe Transitions. In *25th Annual International Conference on Digital Government Research (DGO 2024), June 11–14, 2024, Taipei, Taiwan*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3657054.3657114

DGO 2024, June 11–14, 2024, Taipei, Taiwan

ACM ISBN 979-8-4007-0988-3/24/06
https://doi.org/10.1145/3657054.3657114

1 INTRODUCTION

Critical information infrastructures are vital for many aspects of our societies. With ever-increasing dependencies on the provision of data and services over networks, critical information infrastructures not only facilitate digital communication and information sharing but also support services of other critical infrastructures such as traffic control, internet services, border control financial services [1-4]. For governments, there is a great level of complexity in maintaining their long-lived infrastructure assets and managing established governance of multiple organizations to facilitate the infrastructures [5-7].

In order to prevent potential service disruption and ensure the reliability of services provided by these infrastructures, addressing security issues is considered a crucial and recurrent task [8, 9]. However, protecting the infrastructures against security threats introduced by quantum computers may be unlike the previous continuous control and maintenance efforts. Organizations need to modify their cryptographic layers, which act as the fundamental building blocks of infrastructures. It has been estimated that modifying current cryptographic algorithms to quantum-safe (QS) ones is a complex process that is estimated to take more than a decade [10, 11].

In addition, many uncertainties surrounding the topic of QS transition hinder organizations from their preparation. From the availability of QS technology, direction and time of transition, fragmented standards and protocols, and lack of regulatory clarity to limited resources, uncertainties pose challenges across technological, organizational, and ecosystem contexts [12-14]. Although many public and private organizations are responsible for specific roles in facilitating critical information infrastructures, it is unclear to organizations what should be done and what they need to do for QS transition. Likewise, QS governance among inter-organizations remains unclear, and there is hardly any research on the roles of QS transitions.

Consequently, the topic of QS transition is poorly understood, and we have yet to pinpoint the roles and responsibilities of governments. In this paper, we explore the roles for government in QS transitions and how governments may direct and support organizations in realizing QS information infrastructures. The structure of the paper is as follows: section two lays the background of QS transition and addresses the need for organizations to be adaptive in the face of uncertainties. Section three presents the research methodology and research questions used in this paper. Section four presents and discusses the results gathered from the workshop and interviews. Section five concludes this paper with an overview of the results, limitations, and directions for future research.

2 BACKGROUND

2.1 The need to prepare for Quantum-safe transitions

Recently, IBM announced the first quantum processor with more than 1000 qubits, a significant milestone in quantum computing [15]. Quantum computing offers unprecedented possibilities for solving complex problems (e.g., finding new medicines and logistical optimization). However, this development also challenges the security of widely used encryption algorithms (e.g., RSA and SHA). One of the most well-described threats is Shor's algorithm, which can efficiently factorize large integers [16]. This is a significant concern because many widely used cryptographic algorithms, such as RSA, rely on the difficulty of factoring large numbers for their security.

If a large enough quantum computer becomes available, it could break these encryption methods, compromising the security of sensitive data. Many information infrastructures in the public and private sectors depend on these cryptographic algorithms for several security functions, including user authentication, signing, hashing and communication encryption. In response to the quantum threat, the National Institute of Standards and Technology (NIST) is currently developing QS solution standards [17, 18]. Transitioning to these algorithms is necessary to maintain the security of information infrastructures in a post-quantum era.

2.2 The complexity of Quantum-safe transitions

The complexities of QS transitions require careful planning and coordination to ensure a smooth migration. In 2022, the White House published the preparatory steps for QS transition, and the European Commission announced a call for the Horizon Europe Framework Programme on QS transition [19, 20]. Likewise, the German Federal Office for Information Security (BSI) and the Dutch General Intelligence and Security Service have published the guideline manual for QS transition [21-25]. Yet, modifying current infrastructures with QS technology is unlike previous transitions (e.g., transition to elliptic-curve cryptography, transition from SHA1 to SHA2) [26, 27].

While the future standards of QS cryptographic algorithms are not readily available, modification in the current infrastructures can potentially introduce interoperability and backward compatibility issues [17, 18, 28, 29]. Due to technological interdependencies in the infrastructures, QS transition may need to be carried out across the boundaries of organizations [13]. Likewise, combining current cryptographic algorithms with post-quantum cryptographic algorithms is a novel challenge, demanding organizations to collaborate on which kind of hybrid cryptography will be implemented in a sector or society.

However, a slow change and reactive preparation for QS transition may be insufficient to secure critical information infrastructures for two reasons. First, quantum computing technology is advancing in parallel to the preparation for QS transition, which is estimated to take 10+ years [30, 31]. If QS transition preparation takes longer than the availability of a powerful enough quantum computer, infrastructures will no longer be protected and will become obsolete. Second, data with long-term security needs will become vulnerable to *Store Now, Decrypt Later* attacks, where data can be stored now and decrypted once a quantum computer becomes available [29, 32].

2.3 Roles for government in Quantum-safe transitions

Changes in the existing systems can result in potential delays and failures due to restrictions from the established patterns of decision-making and institutional arrangements [33-38]. From enacting regulations and implementing strategic planning and policy changes to fostering public-private partnerships, governments can fulfill several roles when securing control and managing critical infrastructures [34, 39]. In order to adapt to changing environments, collaboration can occur beyond the boundaries of government to stimulate innovation and establish decision-making and capability mobilization [35, 40, 41]. However, the intertwinement of technology and policies that facilitate the infrastructures is highly regulated and complex, leading to the possibility of a *Catch-22* Loop [34, 35].

Unlike the previous continuous control and maintenance efforts, QS transition involves new technologies with QS cryptographic algorithms. While QS technology is not yet available for organizations to implement and adopt in the existing infrastructures, it may be difficult to change with a set of roles, security policies, encryption mechanisms and procedures that are already in place [34, 42-17, 18, 29, 44, 45]. Due to the far-reaching societal implications of the quantum threat, governments may actively set the conditions and provide guidance for QS transitions [4, 46]. However, while organizations may be waiting for policies and regulations to adopt new QS technology, policymakers may also be waiting for QS technology to be ready [2, 13]. Organizations face a dilemma in identifying "what should be done first," and delays in one challenge can potentially lead to delays in other challenges, leading to a *Catch-22* loop.

Amidst uncertainties, understanding the concept of roles may help clarify what should be done and what organizations need to do. By delineating roles and responsibilities, organizations may better navigate complex situations. Several scholars have studied the concept of roles in a cross-agency process, technology, inter-organizational collaboration and web service orchestration [47-41, 50] and roles in the innovation process and innovation ecosystem [51, 52]. Other literature discusses the roles of government in different technologies such as the adoption of cloud computing [53], the market for electric vehicles [54], and the energy alliance network [55]. While much of these literature do not provide an explicit list of roles, exceptions apply for Guenduez and Mettler [56] as they identify four government roles such as enabler, leader, regulator, and user in the context of AI adoption, and Janssen, Gortmaker & Wagenaar [57] also presents the list of eight different government roles using the example of governmental cross-agency process in web service orchestration.

Going forward, at the time of writing there has been no academic research examining the roles for government in QS transitions. Although Guenduez and Mettler [56] and Janssen et al [57] provide examples of different government roles, we aim to focus on actions needed in the context of QS transitions and examine on how governments can direct and support organizations in realizing QS

information infrastructures. Looking to fill this knowledge gap, we start by using the definition of a role proposed by Kendall [58], which is defined as "a position and a set of responsibilities within the overall structure of the system" (p.353). We use the following definition because: 1. Various actors are responsible for facilitating critical information infrastructure. 2. These actors may need to take part in QS transitions to secure the infrastructures. 3. The roles of these actors may need to be allocated for QS transitions due to multiple complexities and uncertainties. By understanding the roles, the focus will not shift towards 'who should do what' but on 'what should be done.'

3 RESEARCH METHODOLOGY

To understand the different roles for government in QS transitions, the following research question has been formulated: *What are the different roles for government in directing and supporting QS transitions?*

Overview of Research Methodology

The topic of QS transition is relatively new, and QS cryptographic algorithms are a new technology. This is an emerging avenue of research in the field of Information Systems and digital government. Since there is no overview of the roles for government that has been examined in the context of QS transitions, the paper sets the foundation for further research on the roles for government that may be relevant when directing and supporting QS transitions. Due to the limited number of persons with the knowledge and expertise, we used a combination of workshops and interviews as the research method.

We conducted a series of workshops to identify and gain insights on the list of actions needed for QS transitions and relevant roles for governments. With the results gained at the workshops, additional interviews were conducted with practitioners from supervisory agencies that are managing and monitoring critical information infrastructures in the Dutch government. The purpose of the interviews was to extend the discussion on the results of the workshop and gain insights into the practical feasibility of different actions that can be fulfilled by governments. After examining the results from both workshops and interviews, researchers saw different roles emerge and used descriptions of each action to further categorize different roles for governments. The details of workshops and interviews are described in Section 3.1 and Section 3.2.

3.1 Workshops

The use of a workshop as a research method allows researchers to collect data and engage participants in a discussion of an issue or question outside the literature [59]. Three workshops were organized between June 2023 and November 2023. Since there were only a few experts in the area of QS transition, we organized three workshops, and participants were invited to participate on a voluntary basis. The invitation was extended to participants with either a prior technical background or relevant knowledge and experience from industry, government or academia.

The first two workshops were held at the Quantum Meets Event on 14 June 2023. The event was organized by Quantum Delta NL to foster collaboration and learning on the latest research and development regarding quantum technology. By extending the discussion and sharing insights with practitioners and experts, the workshops provided an interactive environment for collaboration and a better understanding of the practical environment. Different participants from government agencies, service providers, software companies, research institutes, tax offices, and banks joined the workshop. During these workshops, participants were asked to identify actions needed for QS transitions.

The third workshop was held at the PKI consortium on 7 November 2023. The event was organized by the Public Key Infrastructure Consortium to discuss the security of the Internet and engage organizations such as users, regulators and supervisory bodies to share knowledge on trusted digital assets and communication. There were 31 participants at the workshop, and the breakdown of participants is shown in Table 1. During the workshop, participants used Mentimeter to share whether they agreed or disagreed with the list of actions needed for QS transitions that are relevant for the government. After examining the results of the list of actions that may be relevant for governments in directing and supporting QS transition, researchers took the list of actions and categorized them into different roles.

3.2 Interviews

We then conducted semi-structured interviews to extend the discussion on the results obtained from the workshop and gain insights on the practical feasibility of the list of actions that were found to be relevant for governments. By conducting additional semi-structured interviews, researchers can acquire in-depth information from respondents and maintain the focus of the study [60]. We interviewed supervisory agencies that manage and monitor critical information infrastructures in the Dutch government. The respondents for the interviews were from Logius and the National Inspectorate for Digital Infrastructure (Rijksinspectie Digitale Infrastructuur), who held prior knowledge of critical information infrastructure and were familiar with the topic of QS transition.

We focused on Logius and the National Inspectorate for Digital Infrastructure because both organizations have the responsibility of maintaining the security of critical information infrastructure in the Netherlands. Logius acts as Policy Authority (PA) and manages the data exchange system in the Dutch government (e.g., PKIoverheid) under the Ministry of Internal Affairs and Kingdom Relations [7, 61–63]. National Inspectorate for Digital Infrastructure, previously known as Agentschap Telecom, monitors both public and private organizations to determine whether they are in compliance with international and EU regulations and legislation [64].

4 RESULTS

From the results obtained from the workshops and interviews, researchers derived the 12 roles for government in the context of QS transitions. The list of 12 roles shows that there are many possible roles that may be needed for QS transitions, and modifying the existing infrastructures with QS technology is complex. While the results provide organizations with an overview of what should be done and what they need to do for QS transitions, they also show that there is a need for intensive collaboration among the organizations to execute different roles, which sets the foundation

Table 1: Number of Participants at the Public Key Infrastructure Consortium Workshop

Number of Participants	Types of Actors
8	Government Agency
1	Standardization Body (e.g., NIST, ETSI, etc.)
11	Private Sector (Service Provider)
4	Infrastructure Solution Provider
7	Academic Institution

Table 2: Possible Government Roles in QS Transitions

Roles	Description
1. Facilitation	Establishing a steering committee and working groups for QS transitions
2. Policies & Regulation	Developing and setting up policies and regulations that support QS solutions
3. Monitoring & Auditing	Establishing monitoring and enforcement mechanisms to review and check QS solutions
4. Coordination	Preparing QS transitions, securing funding and setting up a testing environment for QS solutions
5. Assessment	Conducting impact and risk assessments and identifying areas where QS solutions are needed
6. Standardization	Selecting QS solutions that are based on NIST and validated through testing
7. Implementation	Planning and implementing QS solutions (e.g., identifying key features, functionalities, solution requirements, etc.)
8. Ecosystem Planning	Identifying areas that need collaboration and developing ecosystem-wide transition paths
9. Awareness	Sharing the potential benefits of QS technology and raising societal concerns on quantum threats
10. Execution	Ensuring timely preparation and actions for QS transitions
11. Expertise Center	Setting up an expertise center and sharing knowledge about QS transitions
12. Change Process Management	Managing QS transitions and resolving conflicts once QS solutions are implemented

for further research. Table 2 shows an overview of different roles for QS transitions.

With the roles complementing each other and partly overlapping, we clarified and distinguished the roles that may seem similar. For example, we separated the awareness role and the expertise center role. Although both roles involve knowledge sharing, the awareness role focuses on creating awareness about QS transition and stimulating actors to participate in transitions. On the other hand, the expertise center role focuses on building a centralized knowledge base where organizations can potentially share and learn from each other using best practices, tools and resources from various actors in the ecosystem. The details of each role are described below.

- Facilitation

The facilitator role was considered to be the possible role for government in QS transitions. Although discussions on the topic of QS transition are emerging, various public and private organizations also need to take part in QS transitions. While a steering committee can provide a high-level strategy and decision-making authority, working groups can ensure more hands-on tasks for QS transitions. Establishing a steering committee and working groups can ensure cross-organizational collaboration, facilitate communication, and allow knowledge to be shared with different actors in the ecosystem. Government coordination can promote transparency and maintain interoperability across sectors where critical information infrastructure has a significant public impact.

- Policies & Regulation

Developing and setting up policies and regulations for QS solutions was considered another possible role for government in QS transitions. Implementing policy changes and enacting regulations can establish a legal framework at local, national and international levels. The role of policies and regulations can help manage risks and provide guidelines for QS transitions. Additionally, organizations that are in compliance with laws and regulations can be protected. Since governments are accountable for public safety and safeguarding critical information infrastructure, policies and regulations can address issues surrounding quantum threats and promote standardization of QS solutions.

- Monitoring & Auditing

The monitoring and auditing role was considered as a possible role for government in QS transitions. When implementing and adopting QS solutions, it is crucial to review QS technology, address potential concerns and ensure compliance with regulations. Currently, there is no set way to monitor and audit the process of QS transitions. Since governments have the authority to enforce regulatory compliance, monitoring and auditing can maintain order and security during the transitions and help navigate the legal framework to ensure industry standards. Governments can protect critical information infrastructure by evaluating the real-time performance of new technology and optimizing resources for QS transitions.

- Coordination

The coordination role was another possible role for government in QS transitions. Despite many socio-technical predicaments that

may hinder QS transitions, there is a lack of knowledge on how to transition to a QS situation. In order for organizations to work together and collaborate, coordination is needed to manage activities, resources, and communication within the ecosystem. By securing funding, managing collaboration and setting up a testing environment, cross-organizational objectives can be achieved while maintaining the balance between fostering innovation for QS technology and maintaining regulatory oversight.

- Assessment

The assessment role was considered as a possible role for government in QS transitions. Since QS transition is a complex process with multiple actors in the ecosystem, addressing potential challenges, risks, and needs may vary among different organizations. When the impact of quantum threats on organizations' cryptographic assets is unclear, organizations do not know the scope of their transitions. As government involvement ensures regulatory compliance, assessment practices can also be enforced so that organizations can conduct assessments of the existing infrastructures and identify areas that need changes to optimize the process and efficiency of QS transitions.

- Standardization

Selecting QS solutions that are based on NIST and validated through testing is considered as a possible role for government in QS transitions. The selection of industry standards needs to be approved by standardization bodies (e.g., NIST, ETSI, etc.) as these standards can provide a benchmark for security, quality, performance, and a broader scale of acceptance. For governments, systems and technologies need to work together to operate critical information infrastructure. Selecting QS solutions that align with the accepted standards can help maintain interoperability and compatibility of digital communication and information exchange.

- Implementation

The implementation role was considered as a possible role for government in QS transitions. Regarding the technical aspects of QS solution algorithms, organizations need to identify key features, functionalities and solution requirements. Depending on the process of critical information infrastructure, organizations may have specific needs and system requirements for QS solutions. Government oversight can provide regulatory compliance and ensure that the implementation of QS solutions is effectively integrated with various actors in the ecosystem. For governments, fostering interoperability and compatibility of QS solutions can strengthen the reliability and security of critical information infrastructures.

- Ecosystem Planning

Identifying areas where organizations need to collaborate and developing ecosystem-wide transition paths was considered as a possible role for government in QS transitions. Since there is no guidance available for organizations, it is crucial to identify collaboration among various actors in the ecosystem and align goals for the ecosystem-wide transition. Having ecosystem-wide planning beyond technical aspects can allow organizations to respond to changes in technology, markets, and ecosystem stakeholders. Government involvement can address regulatory and compliance to ensure adherence to industry standards.

- Awareness

The awareness creation role was considered as a possible role for government in QS transitions. For organizations undergoing a QS transition with multiple actors in the ecosystem, clear communication and collaboration are needed. Since governments have the responsibility to protect critical information infrastructures and secure the well-being of citizens, creating awareness can highlight the impact of quantum threats and the benefits of transitioning to QS infrastructures. It would be crucial to stimulate industry stakeholders, experts and the public to participate and gain knowledge on QS transitions. This way, governments can communicate the potential benefits of QS technology and address societal concerns about quantum threats.

- Execution

The execution role was considered as a possible role for government in QS transitions. By addressing legal compliance and using incentives and legislation, governments may provide ways to motivate organizations to take part in QS transitions and identify ways in which organizations can contribute to the preparation. Since a large enough quantum computer can make critical information infrastructures obsolete, QS transitions cannot be delayed. The execution role can ensure timely preparation and execute actions for QS transitions so that milestones are met, and delays are prevented.

- Expertise center

Setting up an expertise center and sharing knowledge of QS transitions was considered as a possible role for government in QS transitions. Expertise centers can provide centralized knowledge with various actors in the ecosystem. By engaging industry stakeholders, experts and the public in discussions, knowledge on the topic of QS transition can be widely shared, and organizations can learn from different approaches to QS transitions. For governments, fostering collaboration and collective knowledge networks can help organizations across different sectors replicate the best practices and ensure that organizations have access to the necessary tools, resources, and personnel for QS transitions.

- Change process management

The change process management role was considered as another possible role for government in QS transitions. In order to ensure smooth and coordinated transitions, any disruptions in the processes and services of critical information infrastructures need to be prevented. It is crucial to optimize resources to identify and resolve conflicts that may occur during QS transitions. Once QS solutions are adopted and implemented in critical information infrastructure, the government can provide support to maintain operational efficiency with the overall change management strategies. By addressing issues, organizations can improve the support system and skills necessary for QS transitions.

5 DISCUSSION

While the extensive list of roles provides an overview of what should be done for QS transitions, it also signals that the readiness for QS transitions remains low, and there are many possible roles that are left to be executed. One of the respondents from the government agency stated, "*People are waiting for a solution. They want to know how they should act. Tell me. I wait. If you tell me, then I act. So people are waiting a little bit and hesitating also. They will only act when*

it's necessary." (R1). Another respondent stated that "*government is keeping an eye on QS transition and keeps conversation ongoing.*" (R2). The current situation signals that preparation for QS transitions is at its early stage, and organizations are waiting for guidance. Although many uncertainties can potentially be crystallized as QS transitions evolve, the results of government roles show that potential delays in one role can also lead to more delays in other roles. It may be crucial for governments to start thinking about which of these roles they want to execute and which of these roles they want to allocate to other actors in the ecosystem.

Moreover, the results indicate that governments are held accountable for transitioning critical information infrastructures with the role of facilitator, and the government has a limited role in ecosystem planning. One of the respondents pointed out, "*We should take a lead role in a committee with a lot of people who are involved. It's not only the government but also collaborating with science institutes to create a quantum strategy.*" (R1). Due to the interoperability of critical information infrastructure across sectors, the supporting role of government as a facilitator was considered important. While the government plays an important role in making decisions for government systems, influence across sectors can also be limited outside of the public sector ecosystem. In such a case, another respondent stated, "*Government should not be leading because it's a business responsibility.*" (R2). However, this may also vary depending on the political systems of countries and how critical infrastructures are set up and managed across sectors.

In addition, the list of possible government roles shows the importance of having urgency among actors in the entire ecosystem. Although much of the attention in preparing QS transitions has been focused on the government, there are many actions left to be executed, and QS transitions cannot be handled by the government alone. The government can only execute the standardization role once NIST has finalized the standardization process. The respondent emphasized that this process is "*Not only for us but also for the businesses. This will give a better grip on the situation*" (R2). The respondent emphasized that it is crucial to have collective efforts in the ecosystem to move as a whole. "*NCSC (National Cyber Security Command Agency) plays a very important role in cyber security. We collaborate with the intelligence agencies, and also with a CIO, CTO and CEOs.*" (R1). In order to plan and coordinate QS transitions, many actors in facilitating the infrastructure need to be part of the process.

In a similar vein, organizations may need to consider their business responsibilities and start preparing for QS transitions. One of the respondents stated, "It's a business decision, and the *government is guiding.*" (R2). Although the government is setting the conditions and providing guidance for QS transitions, preparing for QS transitions is a business decision that organizations need to be responsible for. Another respondent stated that despite the unclear direction of QS transitions, there are many things that organizations can do right now. The assessment role of government can still be executed within organizations to address their low level of awareness and urgency. It would be important to ask, "*Which kind of data is very important for you? Which is your crown jewel? And know where your businesses are, and make a risk analysis for that.*" (R1) The respondent also suggested, "*Get in contact with your suppliers. Get in contact with your department that is facilitating the contracts.*"(R1). By doing so, when the moment arrives for QS transitions, organizations will be ready to transition their infrastructures.

Furthermore, the paper does not rush to finalize the list of government roles for QS transitions. Due to ever-changing circumstances for QS transitions, we expect that the list of roles may change over time and may become more specific for the government to execute as QS transitions evolve. Regarding policy and regulation, one of the respondents stated, "*Legally, there is no need to change to QS solutions since there are no laws and formal mandates.*" (R1). Without new policies and regulations, infrastructures will be legally compliant but technically insecure against quantum threats. Also, it would be difficult to monitor and audit organizations for QS transitions. Another respondent emphasized, "*We don't know how it will go in the near future.*" (R2). While governments are responsible for securing critical information infrastructure, many uncertainties put them in a position to monitor the situations of QS transitions. Likewise, QS governance among inter-organizations remains unclear, and many of these roles for QS transitions have not yet been allocated to execute.

6 CONCLUSION

As there is hardly any research on roles for QS transitions, this paper is the first to investigate the open roles for governments in QS transitions. Based on the workshop and interview results, we have identified 12 different roles for governments when directing and supporting QS transitions. The first exploration of government roles shows that there are many possible roles needed for QS transitions. The roles include facilitation, policies & regulations, monitoring & auditing, coordination, assessment, standardization, implementation, ecosystem planning, awareness, execution, expertise center, and change process management. By examining different roles, there is a clearer idea of what should be done, and governments can start thinking about which of these roles they want to execute and which of these roles they want to allocate to other actors in the ecosystem.

In addition, the results indicate that there is a high level of reliance on governments, and organizations are currently waiting for guidance. While it may be true that governments are held accountable for protecting critical information infrastructures, the results also highlight the importance of preparing QS transitions with the entire ecosystem and that collective efforts need to be made. This means that organizations may also need to keep a close eye on the topic of QS transition and be mindful of their business processes by analyzing the risks and impact of transition. Although we expect that the overview of roles may further change over time, it would still be crucial to involve relevant actors in discussions to start aligning the direction of QS transitions.

Furthermore, there are several research limitations that can result in further research. First, this is not a finalized list of roles due to the early stage of QS transitions we are currently at. Although we involved organizations and persons with knowledge of QS transition, new roles might appear over time, and the current roles may also disappear as QS transitions proceed. Second, we expect the

roles to be executed differently depending on the political environment and per country since critical infrastructures are managed in different ways. Third, the boundaries of the roles are not explicit and may overlap with each other. Given the explorative nature of this paper, the list of roles emerged from the results obtained from the workshops and interviews.

Moreover, the paper offers three avenues of research for QS transitions. First, since the paper provides a starting point for the exploration of government roles in QS transitions, it would be worthwhile to dive into how these roles change over time and whether the allocation of roles is similar and different among various countries. Second, there is no blueprint for QS transitions where we can determine what will happen systematically. It is unclear how organizations will evolve and what may be needed for organizations to navigate QS transitions. How can organizations improve collective urgency and awareness? What are the actions needed in ecosystem-wide transitions? Third, future studies can focus on which of these identified roles will be allocated to whom? And how will they be executed? There are many questions that are left to be explored to further support the upcoming research topic of QS transition.

ACKNOWLEDGMENTS

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).

REFERENCES

[1] Covers, O. and M. Doeland, *How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure.* Journal of Payments Strategy & Systems, 2020. **14**(2).
[2] Kong, I., M. Janssen, and N. Bharosa, Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. Government Information Quarterly, 2024. **41**(1).
[3] Krause, T., *et al.*, *Cybersecurity in Power Grids: Challenges and Opportunities.* Sensors (Basel), 2021. **21**(18).
[4] Lewis, A.M. and M. Travagnin, A Secure Quantum Communications Infrastructure for Europe: Technical background for a policy vision, in JRC Technical Reports. 2022, European Commission.
[5] Chopra, S.S. and V. Khanna, *Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience.* Physica A: Statistical Mechanics and its Applications, 2015. **436**: p. 865-877.
[6] ENISA, Post-Quantum Cryptography: Current state and quantum mitigation. 2021.
[7] Logius, Programme of Requirements part 3: Basic Requirements PKIoverheid. 2022.
[8] Haber, E. and T. Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis.* Florida State University Law Review, 2017. **44**(2).
[9] Tikk, E., Defining Critical Information Infrastructure in the Context of Cyber Threats: The Privacy Perspective. 2018.
[10] Mosca, M., *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* IEEE Security & Privacy, 2018. **16**: p. 38-41.
[11] Mosca, M. and M. Piani, *Quantum Threat Timeline Report 2022.* 2022, Global Risk Institute & EvolutionQ.
[12] Kong, I., M. Janssen, and N. Bharosa, Challenges in the Transition towards a Quantum-safe Government, in Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens, DGO 2022 M.S. In L. Hagen, & S. Hwang (Eds.), Editor. 2022, (ACM International Conference Proceeding Series). Association for Computing Machinery (ACM). p. 282-292.
[13] Kong, I., M. Janssen, and N. Bharosa. *Analyzing Dependencies among Challenges for Quantum-safe Transition.* in *EGOV-CeDEM-EPart2023.* 2023. Corvinus University of Budapest, Hungary.
[14] ToeZine. *Bereid je voor op de dreiging én kansen van kwantumcomputers.* 2023; Available from: https://www.toezine.nl/bereid-je-voor-op-de-dreiging-en-kansen-van-kwantumcomputers/.
[15] Castelvecchi, D., *IBM QUANTUM COMPUTER PASSES CALCULATION MILESTONE.* Nature, 2023. **618**: p. 656-657.
[16] Shor, P.W., Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer. 1994.
[17] NIST, *Report on Post-Quantum Cryptography*, L. Chen, *et al.*, Editors. 2016.
[18] 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.
[19] European Commission. *Transition towards Quantum-Resistant Cryptography.* 2022; Available from: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03.
[20] The White House, *Migrating to Post-Quantum Cryptography.* 2022.
[21] AIVD., *Bereid je voor op de dreiging van quantum computers.* 2021.
[22] BSI, Quantum-safe cryptography-fundamentals, current developments and recommendations. 2021.
[23] Digitale Overheid. *Wat is quantumveilige cryptografie?* 2023; Available from: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/wat-is-quantumveilige-cryptografie/.
[24] NCTV, *Nederlandse Cybersecuritystrategie 2022-2028.* 2022: National Coordinator for Security and Counterterrorism. Ministry of Justice and Security.
[25] TNO., CWI., and AIVD., The PQC Migration Handbook: Guidelines for migrating to Post-Quantum Cryptorgrpahy. 2023.
[26] Amadori, A., J.D. Duarte, and G. Spini, Literature Overview of Public-Key Infrastructures, with Focus on Quantum-Safe Variants Deliverable 4.1, HAPKIDO Project. 2022, TNO.
[27] Bindel, N., *et al.*, *Transitioning to a Quantum-Resistant Public Key Infrastructure.* 2017.
[28] CSIRO, The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography. 2021.
[29] NIST, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, W. Barker, W. Polk, and M. Souppaya, Editors. 2021.
[30] Mosca, M., *Cybersecurity in an era with quantum computers: will we be ready?* 2015.
[31] Mosca, M. and M. Piani, *QUANTUM THREAT TIMELINE REPORT 2020.* 2021, Global Risk Institute.
[32] Mavroeidis, V., *et al.*, *The Impact of Quantum Computing on Present Cryptography.* International Journal of Advanced Computer Science and Applications (IJACSA), 2018. **9**(3).
[33] Anthopoulos, L., *et al.*, *Why e-government projects fail? An analysis of the Healthcare.gov website.* Government Information Quarterly, 2016. **33**(1): p. 161-173.
[34] Bharosa, N., *et al.*, *Challenging the Chain: Governing the automated exchange and processing of business information.* 2015: Logius & Thauris.
[35] Janssen, M. and H. van der Voort, *Adaptive governance: Towards a stable, accountable and responsive government.* Government Information Quarterly, 2016. **33**(1): p. 1-5.
[36] Janssen, M., H. Voort, and A.F. van Veenstra, Failure of large transformation projects from the viewpoint of complex adaptive systems: Management principles for dealing with project dynamics. Information Systems Frontiers, 2014. **17**: p. 15-29.
[37] Mazzucato, M., *Mission-oriented innovation policies: challenges and opportunities.* Industrial and Corporate Change, 2018. **27**(5): p. 803-815.
[38] Meng, J.-H., J. Wang, and Y. Liu, *How is government embedded in innovation process for breakthroughs? A meta-synthesis of qualitative case studies.* Technological Forecasting and Social Change, 2023. **194**.
[39] NCTV, *Resilient critical infrastructure.* 2018: National Coordinator for Security and Counterterrorism. Ministry of Justice and Security.
[40] Chaffin, B.C., H. Gosnell, and B.A. Cosens, *A decade of adaptive governance scholarship: synthesis and future directions.* Ecology and Society, 2014. **19**(3).
[41] Janssen, M. and E. Estevez, *Lean government and platform-based governance—Doing more with less.* Government Information Quarterly, 2013. **30**: p. S1-S8.
[42] CCC, Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. 2019, Computing Community Consortium.
[43] Hunt, R., *Technological infrastructure for PKI and digital certification.* Computer Communications 2001. **24**(2001): p. 1460-1471.
[44] Linn, J., *Trust Models and Management in Public-Key Infrastructures.* 2000.
[45] 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.
[46] Lewis, A.M. and M. Travagnin, The Impact of Quantum Technology on the EU's Policies Part 2: Quantum Communications from Science to Policies. 2018, European Commission.
[47] Bryson, J.M., B.C. Crosby, and M.M. Stone, *Designing and Implementing Cross-Sector Collaborations: Needed and Challenging.* Public Administration Review, 2015. **75**(5): p. 647-663.
[48] Gasco-Hernandez, M., J.R. Gil-Garcia, and L.F. Luna-Reyes, *Unpacking the role of technology, leadership, governance and collaborative capacities in inter-agency collaborations.* Government Information Quarterly, 2022. **39**(3): p. 101710.

[49] Gil-Garcia, J.R., *et al.*, Characterizing the importance of clarity of roles and responsibilities in government inter-organizational collaboration and information sharing initiatives. Government Information Quarterly, 2019. **36**(4).
[50] Hagel, J., *Leveraged growth: expanding sales without sacrificing profits.* Harvard Business Review, 2002. **80**(10): p. 68-77.
[51] Dedehayir, O., S.J. Mäkinen, and J. Roland Ortt, *Roles during innovation ecosystem genesis: A literature review.* Technological Forecasting and Social Change, 2018. **136**: p. 18-29.
[52] Markham, S.K., *et al.*, *The Valley of Death as Context for Role Theory in Product Innovation.* Journal of Product Innovation Management, 2010. **27**(3): p. 402-417.
[53] Ali, O. and V. Osmanaj, *The role of government regulations in the adoption of cloud computing: A case study of local government.* Computer Law & Security Review, 2020. **36**: p. 105396.
[54] Li, S., *et al.*, *The Role of Government in the Market for Electric Vehicles: Evidence from China.* Journal of Policy Analysis and Management, 2022. **41**(2): p. 450-485.
[55] Peterman, A., A. Kourula, and R. Levitt, *Balancing act: Government roles in an energy conservation network.* Research Policy, 2014. **43**(6): p. 1067-1082.
[56] Guenduez, A.A. and T. Mettler, Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies? Government Information Quarterly, 2023. **40**(1): p. 101719.
[57] Janssen, M., J. Gortmaker, and R.W. Wagenaar, *WEB SERVICE ORCHESTRATION IN PUBLIC ADMINISTRATION: CHALLENGES, ROLES, AND GROWTH STAGES.* 2006.
[58] Kendall, E.A., Role Model Designs and Implementations with Aspect-oriented Programming. 1998.
[59] Inmark, *Concept and methodology of Interactive Workshops.* 2010.
[60] Schmidt, C., *The Analysis of Semi-Structured Interviews.* , in *A Companion to Qualitative Research*, U. Flick, von Kardoff, E. and Steinke, I., Editor. 2004, Rowohlt Taschenbuch Verlag GmbH: Reinbek bei Hamburg, . p. 253-259.
[61] Innovalor, PKIoverheid: Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling. . 2019.
[62] NCSC, *PKIoverheid is changing.* 2020, National Cyber Security Center, Ministry of Justice and Security.
[63] SSC-ICT. *Jaarverslag SSC-ICT 2018.* 2018; Available from: https://www.ssc-ictspecials.nl/jaarverslag-ssc-ict/2018/01.
[64] Rijksinspecties. *National Digital Infrastructure Inspectorate (RDI).* 2023; Available from: https://www.rdi.nl/over-ons/documenten/publicaties/2021/12/16/ons-werk.