Policy guidelines to facilitate collective action towards quantum-safety

Recommended policy guidelines to aid and facilitate collective action in migration towards quantum-safe public key infrastructure systems

Christiansen, Lærke Vinther; Bharosa, Nitesh; Janssen, Marijn

DOI
10.1145/3598469.3598480

Publication date
2023

Document Version
Final published version

Published in
Proceedings of the 24th Annual International Conference on Digital Government Research - Together in the Unstable World

Policy guidelines to facilitate collective action towards quantum-safety

Recommended policy guidelines to aid and facilitate collective action in migration towards quantum-safe public key infrastructure systems

Lærke, L, Christiansen*
Faculty of Technology, Policy, and Management, Delft University of Technology
l.v.christiansen@tudelft.nl

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

Marijn, M, Janssen
Faculty of Technology, Policy, and Management, Delft University of Technology
M.F.W.H.A.Janssen@tudelft.nl

ABSTRACT

As the development of quantum computers advances, actors relying on public key infrastructures (PKI) for secure information exchange are becoming aware of the disruptive implications. Currently, governments and businesses employ PKI for many core processes that may become insecure or unavailable when quantum computers break the cryptographic algorithms foundational to PKI. While standardization institutes are currently testing quantum safe cryptographic algorithms, there are no globally agreed-upon cryptographic solutions available. Actors looking to prepare for the implementation of quantum safe cryptographic algorithms lack methods that allow for collective planning and action across organizations, sectors, and nations. The goal of this policy paper is to elicit requirements for a serious game on QS PKI, and derive policy guidelines that actors can use to prepare and formulate governance arrangements. We followed a two-step approach, drawing on technology threat avoidance theory and collective action theory, followed by empirical grounding through a focus group. The results from the literature confirm that a serious game could be a suitable governance mechanism for QS PKI. The focus group results discussed 12 requirements and the requirement's relation to the theoretical background. From this, the findings section arrived at four policy guidelines derived from the requirements that can function as focus areas for further requirement development and as input for policy makers. The policy guidelines concluded are (1) prioritize increasing collective awareness through emphasizing social networks, (2) acknowledge the interdependencies in migrating towards QS PKI, (3) create an understanding of the technical standards in the field and their issuers, and (4) being highly realistic with both negative and positive scenarios to center the players' understanding of real-world impact.

*Corresponding author

DGO 2023, July 11–14, 2023, Gdańsk, Poland

ACM ISBN 979-8-4007-0837-4/23/07.
https://doi.org/10.1145/3598469.3598480

CCS CONCEPTS

• **General and reference** → General conference proceedings.

KEYWORDS

Collective action, Serious Games, Policy, Quantum-Safe PKI, Cybersecurity

ACM Reference Format:

Lærke, L, Christiansen, Nitesh, N, Bharosa, and Marijn, M, Janssen. 2023. Policy guidelines to facilitate collective action towards quantum-safety: Recommended policy guidelines to aid and facilitate collective action in migration towards quantum-safe public key infrastructure systems. In *24th Annual International Conference on Digital Government Research - Together in the unstable world: Digital government and solidarity (DGO 2023), July 11–14, 2023, Gdańsk, Poland.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3598469.3598480

1 INTRODUCTION

The development of quantum computers is rapidly progressing; while companies such as IBM and Google have already made great strides in developing operational quantum computers, we have yet to see a quantum computer strong enough to run Shor's algorithm for prime factorization. However, some researchers argue we will be able to see this kind of development within the next ten years [8, 9]. This is particularly a concern for public key infrastructure (PKI) systems as these make up the majority of encryption schemes for online data communication. PKI systems use two-key asymmetric encryption to ensure the safe communication of data, using what is called a public key to encrypt data that can then only be decrypted by the person with the private key. However, quantum computers pose a threat to our current data security methods because of their unique nature. Since quantum computers can assume a superposition to the binary that current computers rely on for encryption schemes, it practically means a quantum computer can break through encryption in real-time or hackers can use the store-now-decrypt-later method to harvest large quantities of high-importance data that does not diminish in value with time [10]. This is known as the quantum treat. PKI systems are ubiquitous and used by public agencies, banks, healthcare providers, insurance providers, energy infrastructures, cyber-physical infrastructures, and even defense systems rely on PKI systems. Consequently, the scope of potential impact is huge. Recently, U.S. President Joe Biden signed the 'Quantum Computing Cybersecurity Preparedness Act', encouraging the federal government to adopt technology that is

protected from decryption by quantum computing [17]. The law is designed to secure the federal government systems and data against the threat of quantum-enabled data breaches, ahead of 'Q Day' – the point at which quantum computers are able to break existing cryptographic algorithms. Other countries are expected to follow soon. However, transitioning to quantum safe or resilient digital infrastructures is a major challenge. The ecosystem of hardware, software and actors that must prepare is enormous and does not obey national borders, regulations and institutions [13]. Moreover, since there are no ready-to-use, off-the-shelf cryptographic solutions available, it is difficult for actors to start with a transition towards quantum-safe (QS) PKI. When it comes to preparation, serious gaming can be a valuable instrument and likewise has a proven track record with policy making [5, 7]. Yet, there is no academic research on what a useful serious game should look like or what the real-world impact of such a game could look like. Moreover, there is hardly any use of theory for the policy and governance aspects of reaching quantum-safety, and so this paper contributes with the application of two theories on the topic. Accordingly, the main goal of this paper is to investigate requirements for a serious game on QS PKI and combined with expert input arrive at a set of policy guidelines for facilitating collective action for organizations and institutions to migrate toward QS PKI. This will be achieved through the following research question: What are the policy guidelines for facilitating collective action in moving towards QS PKI? Thus the scope of the paper is to assess the issue from a governance perspective, meaning a higher macro and meso level perspective, rather than a managerial, micro level perspective. This means that the paper is not immediately concerned with the transition of the individual organization, but rather how there can be facilitated a transition for whole sectors.

This paper proceeds as follows. Section 2 presents the research approach. Section 3 presents the theoretical background for formulating preliminary requirements as input for a focus group with experts. Two different theoretical foundations were employed: technology threat avoidance theory (TTAT) [11] and collective action theory (CA) [16]. Technology threat avoidance theory provides a useful lens for understanding users' responses to technological threats (i.e. quantum computing) and provides perspectives on how to approach the subject in a manner conducive to inspiring action. Collective action provides a lens for studying interdependencies, as well as providing useful context on how shared resources (i.e. PKI systems) can be sustainably governed. Section 4 presents the results of a focus group with stakeholders from the government sector, as well as stakeholders from the research sector, working on developing the QS PKI. Section 5, condenses the findings of section 4 and considers how they can be translated into policy guidelines. Finally, this paper concludes with four policy guidelines derived from the requirements and literature, that represent pressing elements in the transition process.

2 RESEARCH APPROACH

In order to answer the research question, this paper follows a two-step approach. First, we select a theoretical lens that allows for the identification of preliminary or expected requirements for a serious game. We draw on TTAT and CA to create a perspective that allows for an individual-level understanding of how to motivate action on both the individual and group level. Next, we conduct a focus group that reflects on the preliminary requirements. The data used in this paper was collected from a focus group that was held in December 2022. This focus group took place online, and was held simultaneously on a video call and on a Miro board. On the board participants rated requirements 1 (fully disagree) – 5 (fully agree), and attached notes to their ratings. Then these notes and ratings were discussed together as a group in the video call, creating multiple layers of discourse.

2.1 Expert participation selection

The participants of the focus group were selected based on a set of criteria meant to identify experts who were best positioned to offer critical insight into the topic. The list of criteria prioritizes people possessing an intersection of knowledge from the following topics:

- Knowledge of PKI
- Awareness of the Quantum Threat
- Participants must represent sectors that rely on PKI systems
- Participants must have experience in implementing and integrating new technologies and facilitating change in organizations and institutions.

The participants did not have to fulfill every criterion but were chosen to represent an intersection of experts in the field. The two main criteria were knowledge of PKI and knowledge of the quantum threat, which, as can be seen in Table 1, was fulfilled by all of the experts. From thereon, there was a fairly even distribution between experts representing sectors that rely on PKI systems and experts with experience in implementing and integrating new technologies. There was one expert who fulfilled all four criteria. There was for the majority of the focus group, eight experts present; however, by the end, the number reduced to seven participants. This was due to time constraints from one participant, and it is reflected in the data presented in Table 1.

2.2 Requirement selection criteria

For the selection of foundational requirements, we draw on two theories, technology threat avoidance theory and collective action theory. For both of these theories we reviewed literature where the theories were combined with serious gaming for an empirical perspective. Secondly, the paper has relied on the input and considerations of the experts in the focus group to assess the relevance and appropriateness of the requirements selected. By considering the requirements' average score on a scale of 1(fully disagree) to 5(fully agree), as well as the discussions that were had on them in the focus group, the most relevant requirements were selected. Through this approach, it was also possible to detect general themes within the requirements that made it possible to group certain requirements together as they touched parts of the same topic. An example of one such topic is the interdependencies in the migration process, where the focus group was instrumental in establishing how many of these interdependencies should be included in the game and how much detail it was to be portrayed in.

Table 1: Division of participants

	Knowledge of PKI	Awareness ofthe Quantum Threat	Represents a sector that relies on PKI	Experience in implementing and integrating new technologies and facilitating change in organizations and institutions
Expert 1	1	1	1	0
Expert 2	1	1	1	1
Expert 3	1	1	0	0
Expert 4	1	1	0	0
Expert 5	1	1	0	1
Expert 6	1	1	1	0
Expert 7	1	1	0	0
Expert 8	1	1	0	1

3 THEORETICAL BACKGROUND

Technology threat avoidance theory and collective action theory were chosen to cover the different perspectives of the game's ambition. Namely to facilitate an individual-level understanding of how to motivate action in social actors and how to facilitate action amongst collective groups. These perspectives were chosen with the stakeholders in mind. This game seeks to facilitate collective action for organizations and institutions to migrate to a QS PKI system, but it is important to note that while the ambitions of the game exist on a macro level, organizations and institutions do not play games; people do. Therefore the only way to encourage collective action is to aim at the individuals who make up these organizations and institutions and attempt to communicate the urgencies to them in a manner that resonates with them and inspires action. Furthermore, technology threat avoidance theory and collective action both share a normative understanding of human behavior, which serves as a foundational link between the two theories. This connection allows for a solid combination of the two through highly compatible ontologies.

3.1 Technology Threat Avoidance Theory

Technology Threat Avoidance Theory (TTAT) was originally proposed in 2009 by Liang and Xue and is an amalgamation of health sciences, psychology, information systems, and risk analysis. It is meant to function as a theory that explains technology users' threat avoidance behaviors, which in this instance, means that instead of focusing on how users adapt to potential threats, it focuses on how users seek to avoid them. This is relevant to the matter at hand as many of the solutions for 'Q-day' are focused on avoiding the issue all together, rather than adapting to it after the fact. 'Q-day' is not an inevitability, but something that can be avoided through the right type of avoidance. Liang and Xue argue that there are two cognitive processes that are used to assess potential threats and how to avoid them, and those are threat appraisal and coping appraisal. This will ultimately result in the choice between problem-focused coping or emotion-focused coping, where we seek to target problem-focused coping. Within TTAT, it is argued that the user will decide their coping strategy based on three safeguarding measures 1) the effectiveness of the measure, 2) the cost of the measure, and 3) the user's self-efficacy in taking the measure. One of the central themes of TTAT is that if the user perceives the potential threat to be avoidable through the safeguarding measures and that those safeguarding measures are manageable, they will be motivated to avoid the threat actively. Otherwise, they will try to passively avoid the threat if they don't believe any of the safeguarding measures are accessible to them. As such, the requirements presented in section 4 seek to promote effectiveness, self-efficacy, and modes of managing the cost of transitioning.

We know from previous studies that serious gaming is a useful tool for emergency preparedness [5], and there are studies linking TTAT and serious gaming proving that a gamified approach's ability to create feelings of self-efficacy in players [1]. According to previous studies, this can be achieved by increasing awareness of relevant vulnerabilities and fostering a better understanding of a subject. This hinges on leveraging different types of knowledge, such as observational knowledge, heuristic knowledge, and structural knowledge [9]. Furthermore, as mentioned previously, self-efficacy and serious gaming show that games can be a very useful tool for creating feelings of self-efficacy in players [1–3]. One study investigated how a serious game could create self-efficacy when self-learning disaster strategies, and found that the players' knowledge and understanding was significantly increased by the end of the game, as well as their perceived self-efficacy to employ disaster strategies in real life [3].
From the literature on TTAT, we arrived at three preliminary requirements for the serious game:

(1) Promoting self-efficacy was added as a preliminary requirement, through emphasizing knowledge sharing and social networks.
(2) Prioritizing methods that appeal to problem-focused coping, like striking a balance between positive and negative scenarios to create urgency around the situation, but still making it seem manageable to the player.
(3) Adding an element of governance in the game, to help the player practically understand their positionality in the governance structure, and what moves they are in a position to make. Thereby increasing their understanding of their potential effectiveness.

These requirements form a baseline for the focus group. First, we proceed with elicitating requirements from collective action theory perspective.

3.2 Collective Action

Collective Action (CA) theory focuses on how social actors work together to achieve a common goal. CA does this by arguing that rational social actors often assess the actions of other social actors to inform their own decisions. This act of 'assessing' is what is called collective awareness, and it is the vital first step in the process toward collective action. CA is most famously employed by Nobel laureate Elinor Ostrom to study ecological issues and how the earth's wealth of shared goods can best be governed sustainably. Generally, there are considered to be eight principles of self-governing of shared goods [12], namely:

- Clear boundaries for users and resources
- Accordance between costs and benefits
- Procedures for rule-making
- Both users and the condition of the resources are frequently monitored
- Graduated sanctions
- Mechanisms for conflict resolution
- Minimal recognition of rights by the government
- Nested enterprises [12]

When looking to the governing of QS PKI, we can see that multiple of these principles has yet to be addressed. For example, there have been established no accordance between cost and benefit of QS PKI. While organizations and institutions are becoming increasingly aware that they will have to migrate to a QS platform in the future, it is very unclear how to facilitate the migration process, how much it will cost, what the various types of cost when transitioning will be, and what exactly it will mean to be 'quantum safe'. Likewise there is an apparent lack of clear boundaries for users and resources, procedures for rule-making, and graduated sanctions.

Digital infrastructures constitutes a unique sphere for studying collective action. It opens up for seeing new tendencies in the traditional patterns that have been established in collective action so far. As such, we might understand 'the commons' in regards to digital infrastructure as not a physical space or physical wealth of shared goods but rather as the "shared global infrastructure" [19]. Society has become so reliant on the internet and its digital infrastructures that should our modes of access become degraded or hindered, it would result in a severe disadvantage for the global society. If the secure pathways we rely on for our most important digital communications become unsafe, our entire digital infrastructure becomes unstable and will only exacerbate the degradation of international cybersecurity. Therefore it is important to research how collective action can be facilitated for issues relating to international cyber security, such as QS PKI.

In later years, we have seen CA increasingly being applied to study socio-technical issues [4, 6, 19]. Dejean et al. [6] found in their research on collective action in P2P file-sharing communities that, paradoxically, there was a positive correlation between the size of the community and the amount of collective goods provided. This is paradoxical as it stands in opposition to what Elinor Ostrom argued, namely that smaller communities had a higher propensity for collective goods. The main difference between the studies of Ostrom and Dejean et al. is that Ostrom focused on environmental studies and economics, whereas Dejean et al. focused on a more socio-technical perspective with online communities. Furthermore, Bourazeri & Pitt [6] did a study wherein they researched the initial effectiveness of a game-based approach to facilitating collective action in socio-technical systems. They found that serious games were a highly efficient way to facilitate collective awareness. This could be done by utilizing social networks within the game and implementing a shared space that could promote participation in 'assembling' shared solution solutions. Through these tools, a serious game could indeed promote collective awareness, with the potential for facilitating collective action. From a game development perspective, the most important elements in achieving a state of collective awareness were the game interface and interaction design [4]. Moreover, previous literature on using serious games to promote collective action shows that in the past, games have been successful in facilitating social engagement for collective action [18], increasing the number of communities that self-govern resources [14], and changing attitudes [15]. These are similar issues that the serious games proposed in this paper aim to address.

From CA, we likewise arrived at three preliminary requirements for the game.

(1) Highlighting interdependencies and structures in the field to emphasize the boundaries, benefits, and costs of the transition process.
(2) Prioritizing social networks to create collective awareness, and
(3) Encouraging collaboration between different stakeholders in the process.

Combined. TTAT and CA provide six preliminary requirements for a serious game. These requirements were used as starting point for a focus group on the requirements for a serious game that would help actors prepare for the transition to QS PKI systems. The next section discusses the results of the focus group.

4 FOCUS GROUP RESULTS

As previously mentioned, the selection of requirements focused partly on the distribution of votes for the different requirements, which was then further supported by the discussions had by the group. This allowed for identifying similar themes and traits across multiple requirements and thereby identifying the most relevant traits present in multiple requirements. This is then assessed in conjunction with the preliminary requirements found in theory. Ultimately this leads to four overarching themes that we propose as policy guidelines for future action on transitioning to QS PKI. For the focus group the experts were asked to consider what practical components would be necessary for the user to play game, as well as what elements would be necessary to ensure the quality of the game. This includes considering different levels of integrity and real-world application of the game that had previously been discussed on the practical requirements section.

In Table 2, the requirements are listed from the most agreed with to the least agreed with. This is done to emphasize the range of requirements presented to the focus group, and to provide a well-rounded representation of what the opinion of the experts is.

Table 2: Requirements Derived from focus group

NUMBER (#)	REQUIREMENT FORMULATION	AVERAGE SCORE (1-5)
#1	The game should be (re)playable for multiple phases in the transition process	4
#2	After the game, the players should leave with at least one clear goal to implement in their organization	4
#3	The game should help players decide on what to do with NIST PQC standards	4
#4	The game should expose the interdependencies organizations have when it comes to migrating to QS PKI	4
#5	The game should focus on positive scenarios: How we can use collective action to avoid the quantum threat	4
#6	The game should focus on individual sectors	3
#7	The game should help players determine an effective governance structure towards QS PKI	3
#8	The form of the game should encourage interaction between players	3
#9	The players should have a basic understanding of PKI and the quantum threat	3
#10	The governance structure should be focused on a specific sector to be effective	2
#11	The game should determine a feasible PQC roadmap for the sector	2
#12	Before the game, the player should have at least one idea of what to achieve with the game	2

A requirement that averaged high was for the game to have replayability for anytime in the transition process (#1). Making it possible for the player to play the game at any point in their quantum-journey functions as a tool for promoting action-based coping from the player and helps promote feelings of self-efficacy and effectiveness. Moreover, giving the players the action to come back and replay the game after they start their process will help the player to reposition themselves in the field and be reminded of the relevant social networks and interdependencies in the field. Through this, the player should be able to re-center their knowledge of the transition process and leave with renewed insight. Moreover, the game should be able to assist the player in finding at least one clear goal to implement by the end of the game (#2), as such promoting feelings of self-efficacy. This is particularly important to consider, as even if the change needs to be facilitated within an entire organization, it is not organizations that play games, it is the people within it. Therefore, it is pertinent that the game can create feelings of self-efficacy and action-based coping in players, as it is, in the end, the people of an organization that will facilitate the change necessary. For that, they need to be collectively aware and feel capable of creating sustainable change. However, as we can see from the two requirements most disagreed with, the player needs to be able to come to this game with little to no insight into the topic. Moreover, the game should not be limited to one individual sector but should be broadly available to whoever should like to play it (#10). We can see this confirmed in requirements #3, which argues that the game needs to help the player understand the technical standards in the field and help them understand what the impact of these standards are and why they matter. This is likewise seen in requirement #4, that the game must assist the player in mapping and understanding the interdependencies in the field. This is important for creating collective awareness, as it is through highlighting all the actors in the field that players can become aware of what rational social actors to look to follow. Generally speaking, the game should support some elements of governance for QS PKI, as it is pertinent to help the player understand the interdependencies in the field, why and how technical standards matter, and who the relevant stakeholders and social actors are in the process. However, the experts emphasized a need for a broader view of a governance model in the game, one that went beyond a sectoral view. This came from an understanding that the game should be able to reach as wide an audience as possible, and relying on a broader focus also strengthens the player's holistic understanding of what the field realistically looks like.

Overall, we can see that the game calls for accessibility and a direct line to real-world impact. Moreover, the game needs to practically possess an openness that allows for players of a broad range of background to play the game. Likewise, there should be no requirement of prior knowledge, as due to the niche nature of the subject, it would limit the pool of potential players significantly. Furthermore, the game should not provide grand solutions like roadmaps or whole governance models, but rather to show the complexities of the situation and create lasting and impactful insight for the player. This should be done by including a network perspective that highlights elements of soft power and makes the player aware of the full scale of rational actors in the field. With this perspective the player will be in a better position to understand the real-world complexities of migrating to QS PKI.

5 FINDINGS

When considering the coherence between the 12 requirements above, we can start identifying common themes. All of the requirements are interconnected, but they can overall be considered through the lens of these four shared characteristics. The first one being that the game should aim to increase collective awareness by focusing on social networks in the game. Collective awareness is the crucial first step in facilitating collective action. Previous research on serious gaming and collective action shows that the best approach for creating collective awareness is to emphasize social

networks in the game. The second is to highlight the interdependencies in the field. This includes the interdependencies between organizations and institutions, as well as other stakeholders and actors in the field, such as service providers, software vendors, PKI authorities, sectoral standardization bodies, etc. The third is for the game to help the player understand the technical standards and developments in the field. This includes exemplifying what the impact could be for implementing the standards of different standardizing bodies like NIST and ETSI. These are important for the player to understand as standardizing bodies within the field play an important role in testing new methods and laying the groundwork for new protocols for organizations to follow. Lastly, the fourth is that the game should engage the player and center their understanding of the issues through being as realistic as possible and being bound in real-world scenarios. These scenarios should be both positive and negative to help the player understand the full ramifications of migrating to QS PKI. As was established through TTAT, it is important to strike a balance between positive and negative scenarios in order to have the migration process seem feasible and manageable. One way of doing so is by relying on collective action. Encouraging collaboration will increase the players' feeling of self-efficacy, make the cost of the process seem less extensive, and working together will also make the process more effective.

Ultimately these themes can also be considered as policy guidelines for further policy development in the field. The call for emphasizing social networks in the game can be emulated in the real world by providing shared spaces for actors who rely on PKI. As mentioned previously, a multitude of sectors and industries rely on PKI and a lot of progress stands to be gained by encouraging collaboration and emphasizing social networks to facilitate collective awareness. Secondly, highlighting interdependencies is equally crucial in reality as actors need to comprehend that the structures of PKI governance consist of multiple soft-power actors that heavily influence the tendencies and standards of the field. This can be partially accomplished by relying on the social networks emphasized previously, but also by making knowledge on governance and PKI more accessible and approachable, such as through a serious game. Likewise, it is important for future policies on PKI to take into account the soft power actors in the field that plays a significant role in setting protocols and standards in the field, like NIST and ETSI. By highlighting these actors and clarifying their roles in the field, it will also help more people understand where to look for continuous guidance on PKI. Lastly, it is paramount that future policies on PKI rely on use cases to emphasize what real-world application can look like, and thereby lowering the bar for action. These use cases should ideally rely on both negative and positive scenarios to help the user understand the urgency of the matter, but also to make them feel like the preventive measures necessary are achievable and relevant.

6 CONCLUSIONS

This paper is the first to explore requirements for a serious game that allows actors to prepare for the transition to QS PKI. Based on the literature, we can conclude that serious games have the ability to promote different elements of collective action. This includes creating collective awareness, facilitating self-governance of shared resources, changing attitudes on social issues, and creating engagement for collective action through technical and socio-institutional learning. Thus we conclude that a serious game is a suitable tool for promoting collective action in migrating toward QS PKI.

This paper concludes that these four policy guidelines are the most important for policy makers to address when attempting to facilitate collective action in moving towards QS PKI:

- Rely on social networks to facilitate collective awareness of the issue
- Future policies need to acknowledge the various interdependencies there are when migrating to QS PKI, and highlight non-official soft power actors.
- Future policies need to encompass the technical standards in the field, what is needed for implementation, and what the consequences might be if the player should choose not to adopt these standards.
- Policy makers should employ use cases to engage stakeholders and center their understanding; future policies should rely on both positive and negative use cases to encourage awareness and action.

Thus, in conclusion, this paper argues that a serious game can be a suitable tool for promoting collective action for organizations and institutions to migrate to a QS PKI system. Moreover, this paper concludes that the most poignant areas in this transition can be considered as creating collective awareness, highlighting interdependencies, facilitating a technical understanding, and emphasizing real-world impact. However, there are some limitations of the study that needs to be highlighted. The study was conducted in an entirely Dutch context, with Dutch organizations and institutions participating in the focus group. This means that the results are limited to a Dutch context. Nonetheless, the research design that this paper is based on could easily be applied to any other country or international context, if someone should wish to do a similar form of requirement testing for a serious game. Another limitation is the small size of the focus group. Due to the subject sitting at the intersection of two, rather niche subjects, namely, PKI and the quantum threat, the relevant group of participants is inherently small. When this is then combined with the busy schedule of technological experts, it becomes increasingly difficult to get a decisively large group of expert participants together. However, the exclusivity of the subject is another argument in favor of developing a game that would create more awareness on the topic.
Lastly, the four policy guidelines recommended in this paper are meant to function as a basis for the further development of more fine-grained requirements. For future requirement elicitation, these requirements will allow us to narrow down on requirements in four very specific areas, that experts have deemed the most pressing areas to address in the transition to QS PKI.

ACKNOWLEDGMENTS

This research for this paper was funded by the HAPKIDO project as a part of their Governance Track with project number NWA.1215.18.002, partly financed by the Dutch Research Council (NWO).

REFERENCES

[1] Arachchilage, N.A.G. and Hameed, M.A. 2017. Integrating self-efficacy into a gamified approach to thwart phishing attacks. arXiv.

[2] Backlund, P. *et al.* 2008. Designing for Self-Efficacy in a Game Based Simulator: An Experimental Study and Its Implications for Serious Games Design. 2008 International Conference Visualisation (Jul. 2008), 106–113.

[3] Blasko-Drabik, H. *et al.* 2013. Investigating the Impact of Self-Efficacy in Learning Disaster Strategies in an On-Line Serious Game. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 57, 1 (Sep. 2013), 1455–1459. DOI:https://doi.org/10.1177/1541931213571325.

[4] Bourazeri, A. and Pitt, J. 2014. Collective Awareness for Collective Action in Socio-technical Systems. 2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems Workshops (Sep. 2014), 90–95.

[5] Chittaro, L. and Sioni, R. 2015. Serious games for emergency preparedness: Evaluation of an interactive vs. a non-interactive simulation of a terror attack. Computers in Human Behavior. 50, (Sep. 2015), 508–519. DOI:https://doi.org/10.1016/j.chb.2015.03.074.

[6] Dejean, S. *et al.* 2010. Olson's Paradox Revisited: An Empirical Analysis of incentives to contribute in P2P File-Sharing Communities. SSRN Electronic Journal. (2010). DOI:https://doi.org/10.2139/ssrn.1299190.

[7] Duke, R.D. and Geurts, J.L.A. 2004. Policy games for strategic management: pathways into the unknown. Dutch University Press.

[8] Grimes, R.A. 2019. Cryptography apocalypse: preparing for the day when quantum computing breaks today's crypto. John Wiley & Sons Inc.

[9] Joseph, D. *et al.* 2022. Transitioning organizations to post-quantum cryptography. Nature. 605, 7909 (May 2022), 237–243. DOI:https://doi.org/10.1038/s41586-022-04623-2.

[10] Kong, I. *et al.* 2022. Challenges in the Transition towards a Quantum-safe Government. DG.O 2022: The 23rd Annual International Conference on Digital Government Research (Virtual Event Republic of Korea, Jun. 2022), 282–292.

[11] Liang and Xue 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly. 33, 1 (2009), 71. DOI:https://doi.org/10.2307/20650279.

[12] Managing the Commons- Eight Principles to Self-Govern: https://serve-learn-sustain.gatech.edu/managing-commons-eight-principles-self-govern. Accessed: 2023-01-12.

[13] Mashatan, A. and Heintzman, D. 2021. The complex path to quantum resistance. Communications of the ACM. 64, 9 (Sep. 2021), 46–53. DOI:https://doi.org/10.1145/3464905.

[14] Meinzen-Dick, R. *et al.* 2016. Games for groundwater governance: field experiments in Andhra Pradesh, India. Ecology and Society. 21, 3 (2016), art38. DOI:https://doi.org/10.5751/ES-08416-210338.

[15] Mota, F. *et al.* 2016. Serious Games as a Tool to Change People Attitudes: An Analysis based on the Discourse of Collective Subject. Literacy Information and Computer Education Journal. 7, (Dec. 2016). DOI:https://doi.org/10.20533/licej.2040.2589.2016.0318.

[16] Ostrom, E. 2009. Collective Action Theory. The Oxford Handbook of Comparative Politics. C. Boix and S.C. Stokes, eds. Oxford University Press. 0.

[17] Coker. President Biden Signs Quantum Cybersecurity Preparedness Act into Law: 2022. https://www.infosecurity-magazine.com/news/biden-quantum-cybersecurity-law/. Accessed: 2023-01-31.

[18] Riar, M. *et al.* How game features give rise to altruism and collective action? Implications for cultivating cooperation by gamification.

[19] Shackelford, S.J. ed. 2020. Managing Cyber Attacks as a Global Collective Action Problem. Governing New Frontiers in the Information Age: Toward Cyber Peace. Cambridge University Press. 87–172.