Quantum Security Threat Discovery

A Value Sensitive Design Approach to Discovering Security Risks of Quantum Sensing at the Port of Moerdijk

Umbrello, Steven; Vermaas, Pieter E.; Kumara, Indika; Alleblas, Joost; Driessen, Stefan; van den Heuvel, Willem Jan

DOI
10.1007/s11569-025-00475-y

Publication date
2025

Document Version
Final published version

Published in
NanoEthics

Nanoethics (2025) 19:8
https://doi.org/10.1007/s11569-025-00475-y

ORIGINAL RESEARCH PAPER

Quantum Security Threat Discovery: A Value Sensitive Design Approach to Discovering Security Risks of Quantum Sensing at the Port of Moerdijk

Steven Umbrello · Pieter E. Vermaas · Indika Kumara · Joost Alleblas · Stefan Driessen · Willem-Jan van den Heuvel

Received: 25 September 2024 / Accepted: 1 June 2025

Abstract This paper investigates the application of *Security Threat Discovery Cards* (STDCs) for identifying security risks in quantum sensing technologies within port security contexts. With the advent of quantum technologies, organizations and stakeholders face the challenge to explore and assess the impact of the applications these technologies will bring. This exploration faces the perceived incomprehensibility of quantum technologies, and suggests a preliminary step aimed at understanding these technologies. Our results suggest that organizations and companies considering the application of quantum technology can skip this preliminary step and independently identify their main risks of quantum applications in a nuanced manner. Our case is an exploration of quantum sensing application by Port security personnel with the STDCs. The research consisted of two independent empirical studies: a workshop with Port of Moerdijk personnel using STDCs and semi-structured interviews with security experts. The comparative analysis of the findings from these studies demonstrates the STDCs' efficacy in revealing with the Port's personnel assessment of nuanced risks beyond the experts' foresight. For example, the interviews with experts raised concerns regarding governance, ethical implications, and the human factor in quantum technology integration. The workshop with personnel not only suggested similar concerns but also uncovered additional risks, including socio-technical threats and broader societal impacts.

Keywords Quantum Sensing Technologies · Security Threat Discovery Cards · Port Security · Risk Assessment · Socio-technical Threats

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s11569-025-00475-y.

S. Umbrello (✉)
University of Turin, Turin, Italy
e-mail: steven.umbrello@unito.it

P. E. Vermaas (✉) · J. Alleblas
Delft University of Technology, Delft, Netherlands
e-mail: P.E.Vermaas@tudelft.nl

J. Alleblas
e-mail: J.Alleblas@tudelft.nl

I. Kumara · S. Driessen · W.-J. van den Heuvel
Tilburg University, Tilburg, Netherlands
e-mail: i.p.k.weerasingha.dewage@tue.nl

S. Driessen
e-mail: s.w.driessen@jads.nl

W.-J. van den Heuvel
e-mail: W.J.A.M.v.d.Heuvel@jads.nl

Introduction

In the early 20th century, the emergence of quantum theory provided the foundations on which existent technologies could springboard into more modern, familiar technologies. The vacuum tube was quickly

Published online: 01 July 2025

replaced by the more reliable and efficient transistor, a commonplace component that marks many contemporary systems [10]. However, this first revolution in how quantum mechanics can be used to create new technologies was limited by our understanding of the theory of quantum mechanics that was, and still is, evolving. We now find ourselves at a new frontier of how quantum mechanics can be harnessed to ever greater degrees of precision, where the technologies exist in delicate quantum states, like in quantum computing (e.g., Gyongyosi and Imre 2020), or how quantum mechanics can manipulate matter at the level of particles, like lasers (e.g., [18]. This appropriation of quantum mechanics to develop new technologies has been termed 'the second quantum revolution' [4].

Not only academics, but also industry leaders and defense sector specialists have understood the potential value of harnessing quantum mechanics directed at improving current technologies and developing novel technologies, given the surge in investment in the burgeoning quantum sector [8, 19]. This hype towards channeling quantum mechanics for the purposes of driving technological innovation has likewise sparked concerns over the ethical, legal, economic, and social implications that these quantum technologies may have [12, 25]. However, correctly addressing these concerns poses a challenge given the nascent state of these technologies as well as a lack of examples of how these technologies go wrong in real-world contexts. At the same time, where lies the problem lies also the solution. The early stages of the development of these quantum technologies provide us with the opportunity to construct the scaffolding on which risks and consequent mitigation strategies can be identified and operationalized [13].

Identifying the risks that may come with quantum technologies requires overcoming two challenges. The first is that applications are not yet well-developed thus obstructing detailed analyses of their impact. The second is that quantum technologies are often perceived as incomprehensible because of the enigmatic nature of the underlying quantum mechanics, thus making stakeholders shy away from analyzing applications. These challenges suggest that before engaging in projects to identify the risks, quantum technologies have to develop into concrete applications, and second, an effort should be made to make quantum technologies comprehensible to all stakeholders [23]. In this paper, we take another approach to these challenges and explore the possibilities for identifying risks of quantum technologies applications when these applications are described in generic functional terms. At the same time, the precise technical and quantum-mechanical details of this functioning are black-boxed. Moreover, to increase the adoptability of the tool, we explore the possibility of applying the principle of subsidiarity[1] to the identification protocol with personnel of organizations or companies that are considering adopting these applications, thus enabling such organizations and companies to carry out the risk identification themselves. The Dutch *Centre for Quantum and Society*[2] has already launched such self-help tools for getting ready for the emergence of quantum technologies, such as the *Exploratory Quantum Technology Assessment* method.[3] More tools are welcome, given the expected wide dissemination of these technologies.

This paper investigates the use of *Security Threat Discovery Cards* (STDCs) to identify security risks associated with quantum sensing technologies in the context of port security. The challenge lies in that quantum technologies are often perceived as too complex and incomprehensible, which can hinder stakeholders from fully engaging in the risk assessment process. To address this, the STDCs offer a novel approach that allows stakeholders to explore security risks without needing to delve into the technical intricacies of quantum mechanics. Through two independent empirical studies—a workshop with personnel from the Port of Moerdijk and semi-structured interviews with security experts—this paper explores how STDCs can facilitate the identification of nuanced risks, including governance, ethical implications, and socio-technical threats. The results suggest that STDCs enable organizations and companies to

[1] The principle of subsidiarity is a political and social philosophy that suggests that matters ought to be handled by the smallest, lowest, or least centralized competent authority. Originating from Catholic social teaching, this principle is grounded in the belief that decisions should be made as close as possible to the grassroots level, allowing for greater participation, accountability, and responsiveness to the needs of the community. This approach ensures that decisions are made by those most affected by them and who have the best understanding of the local context, fostering a sense of empowerment and efficiency.

[2] https://quantumdelta.nl/society-application

[3] https://issuu.com/quantumdelta.nl/docs/eqta_-_english_version

independently assess the risks of quantum technology applications in a comprehensive and nuanced manner, even in the absence of detailed technical knowledge.

The first part of this paper outlines the value sensitive design (VSD) approach to technology design and its application in security threat discovery. The second part details the methodology of using STDCs for risk assessment in quantum sensing applications. The third section presents the findings from the empirical studies, demonstrating the efficacy of STDCs in surfacing security risks. The final section discusses the implications of these findings and provides a preliminary taxonomy of security risks associated with quantum sensing, along with recommendations for future research.

The primary contribution of this paper is a structured assessment STDCs as a tool for identifying security risks in the context of quantum sensing technologies. Rather than merely applying STDCs, this study evaluates their effectiveness in enabling stakeholders to recognize security risks independently without requiring deep technical expertise in quantum mechanics. By integrating conceptual and empirical investigations, we illustrate how STDCs serve as a practical framework for surfacing governance, ethical, and socio-technical risks, thereby offering a replicable approach for future quantum technology assessments. The outcomes of the workshop and interviews were not only of value in testing the efficacy of the STDCs cards for subsidiary exploration of security risks that may come with emerging technologies; they also identified such risks. This paper therefore can also outline a preliminary taxonomy of risks that emerge from the use of quantum sensing, in particular, related to the impact on stakeholders, as well as the reasons, resources, and motivations that could underline adversarial risks to the security of quantum sensing systems.

The first part of this paper outlines the VSD approach to technology design, highlighting its strengths and methods. The second part looks at the STDC toolkit, in particular, discussing how it can be appropriated and applied to quantum sensing to uncover security risks. The third section engages in a conceptual investigation to determine what the current scholarship highlights as the main security issues with quantum sensing. This conceptual investigation is paired with an empirical investigation during which the STDCs were used in a stakeholder event with the Port of Moerdijk authorities as well as independent port security experts to determine the additional risks that could be found with the STDCs. The final section outlines and discusses a taxonomy of security risks discovered in the activity, lists the benefits and shortcomings of employing the STDCs for security threat discovery, and highlights some avenues for potentially fruitful future research.

Value Sensitive Design

As this paper explores the security threats associated with quantum sensing technologies, the adoption of a VSD framework emerges as a pivotal strategy. VSD, with its inherent focus on human values of ethical concern, offers a comprehensive approach to anticipate and address the multifaceted security concerns that quantum sensing technologies present [21]. This design approach is especially relevant given the complex and far-reaching implications of these technologies on various stakeholder groups. In an era where quantum advancements are rapidly evolving, VSD provides a structured methodology to ensure that ethical, societal, and security considerations are not just afterthoughts but integral components of technology design. By employing the VSD framework, this paper aims to unravel the nuanced interaction between quantum sensing technologies and their societal impacts, offering a proactive stance in identifying and mitigating potential security risks.

VSD is philosophically predicated on what is called the *interactional stance* on technology [6]. Historically, technology has been construed as being either a neutral tool (*instrumentalism*), as the force which determines society (*technological determinism*), or as being entirely dependent on society (*social constructivism*). Instead, the interactional stance argues that technology can be understood as all three of those positions. This means that technological systems form a part of society that both determines and is determined by it.

VSD originated within the field of Human-Computer Interaction or HCI. Batya Friedman and colleagues developed the original approach from the University of Washington. As the practice grew more widespread, others developed it (sometimes under somewhat different headings, such as ‘Values at Play’ or ‘Design for Values’ [5, 22]. At the heart

of the VSD approach is what is often referred to as a tripartite methodology of empirical, conceptual, and technical 'investigations'. Whether carried out consecutively, in parallel, or iteratively, these investigations involve (1) empirical investigations into relevant stakeholders, their values, and their value understandings and priorities,(2) conceptual investigations into these values and their possible trade-offs; and (3) technical investigations into value issues raised by current technology and the possibilities for value implementation into new designs.

VSD is a design approach that provides both a theory and method to design *for* human values in a "principled and systematic manner throughout the design process" ([7], p.2). Fundamental to VSD is the focus on the interplay of our technical and moral imaginations concerning salient design features. Although value sensitive design shares a lot of commonalities with other approaches to design like universal design, participatory design, and inclusive design, VSD is characterized by at least seven structural features that make it comparatively unique:

1. VSD is explicit in its anticipatory orientation. It affirms the long-term impacts that technologies have on society and aims to be proactive by centralizing human values early on and throughout the design process.
2. VSD expands the domain of relevant values to loci outside of the design domain. This includes the home, cyberspace, schools, and other areas of public life.
3. Beyond solely economic values, or the democratic values central to approaches like participatory design, VSD expands the domain of relevant values to focus on those values of moral importance.
4. VSD proposed an iterative and reflexive methodology of conceptual, empirical, and technical investigations (discussed further below) that allows it to arrive at greater equifinality over time.
5. VSD is predicated on the *interactional* stance on technology and thus affirms that both technology and social forces exist as a dynamic interplay. Design then must be orientated towards this covariance of technology and society.
6. VSD draws from moral epistemology and affirms that moral values are independent of individuals' beliefs in those values.
7. VSD rejects social or cultural relativism about moral values and instead affirms the independence of certain moral values regardless of socio-ocultural differences. Values like justice, well-being, and dignity are framed as independent, universal moral values in design [6]. Nevertheless, how those values are *actually* manifested can be different due to the various socio-cultural understandings of those values.

As its name suggests, VSD focuses on human values bridging the gap between design and ethics. Values are expressed and embedded in technology; they have real and often non-obvious impacts on users and society. Values are understood in VSD as "what a person or group of people consider important in life," particularly those of moral importance ([7], p.56) (Fig. 1).

As we mentioned, one of the distinguishing features of VSD is its tripartite structure, meaning that it is composed of three iterative and interdependent phases or 'investigations': conceptual, empirical, and technical investigations. They can be carried out consecutively, in parallel, or iteratively and are meant to be in constant feedback with one another to arrive at a salient design. Often many VSD projects begin with *conceptual investigations* which aims to construct working answers and definitions to questions like "what are values?", "who are the stakeholders impacted by these design choices?", "which stakeholder values should be supported in design and at what opportunity cost?", "how do we resolve value tensions and moral overload?", "how and why do certain design choices impact certain stakeholder groups?". Conceptual investigations are often understood as the most philosophically oriented of the three investigations. Here design teams can take up the philosophical literature itself as a starting point in drafting thorough working understandings of those questions, which can then be referred to and refined through the other two investigations.

Stakeholders are central to VSD. When we talk about values, we beg the question: *the values of whom?* VSD is unique in its distinction between two major types of stakeholders: *direct stakeholders* and *indirect stakeholders*. Direct stakeholders are the

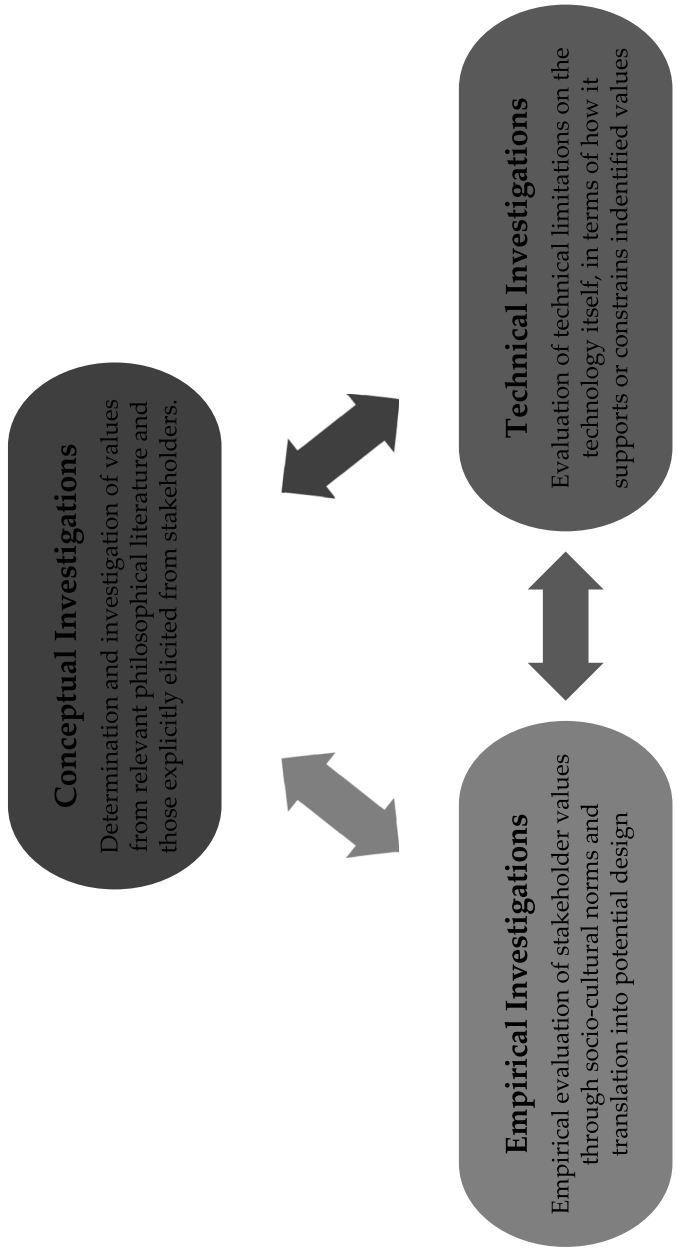

Fig. 1 The recursive VSD tripartite framework. Source: Umbrello [20].

individuals and/or groups that directly interact with the system or its output. A prominent example of direct stakeholders would be the designers themselves who work day-in and day-out with the system and the system users when deployed and diffused. Indirect stakeholders refer to all other entities affected by the use of the system but do not directly interact with it. Indirect stakeholders are often the class of stakeholders who are overlooked in the design of systems. For example, nuclear energy plants have been designed with many direct stakeholders in mind (e.g., energy companies, governments who need to meet sustainability goals, and individuals looking for competitive energy pricing). However, the indirect stakeholders, like nonhuman animals and the surrounding ecosystems that the eventual waste might impact, are often not accounted for. But recall that VSD is also temporally sensitive. This means that stakeholder groups can change over time. Those very same entities that are direct stakeholders today can also be considered indirect stakeholders when designing for multiple generations. If we take the same example, the design of nuclear power implicates companies, governments, and people who need to manage the nuclear waste over many generations.

Security Threat Discovery Cards

One of the seventeen noted tools that fall within the rubric of the VSD approach is *Envisioning Cards*™. The *Envisioning Cards*™ are a set of 32 cards that fall into four different suits: (1) Stakeholders, (2) Values, (3) Time, and (4) Pervasiveness. The cards were designed to raise awareness of long-term and systemic issues in design and are built on more than two decades of value sensitive design research [3],cf. [15].

The *Envisioning Cards*™ are a general tool not geared toward any specific technology or design program. They can be used in various contexts without any rigid guidelines, thus permitting their use to be modified and appropriated to those contexts. Still, there are certain ethical, social, and legal issues that emerge as a consequence of the particulars of technology, thus requiring targeted attention to determine the risks, issues, stakeholders, etc., of that technology. Concerning quantum technologies and security issues raised by those technologies, this is a primary example. In response to security issues more broadly, Denning et al. [3] developed a target set of cards that are intended to help security specialists, designers, and other stakeholders think about computer security threats. The STDCs, which are a deck of 42 cards, are categorized into four dimensions (suits): (1) Human Impact, (2) Adversary's Motivations, (3) Adversary's Resources, and (4) Adversary's Methods (see Fig. 2). Like the *Envisioning Cards*™, the STDCs have template cards for those who wish to make their own for their specific domain of use.[4] Originating from the realm of computer security, STDCs offer a structured and comprehensive framework for uncovering potential risks and vulnerabilities. Their categorical approach is particularly suited to the multifaceted nature of quantum technologies. These technologies, while groundbreaking, introduce complex security challenges that traditional assessment tools may not fully capture. The adaptability and depth of the STDCs allow for a nuanced exploration of these challenges, ensuring that potential threats are not only identified but also thoroughly understood in the context of their impact on both direct and indirect stakeholders.

The STDCs can be used for a wide range of purposes and in a wide range of contexts. For example, the cards could be used by students to learn about security threats, by professional software and hardware developers for training and to surface threats in system design, and by project teams to communicate about potential security threats with management and others. The creators offer two step-by-step activities for using the cards both in an educational and training context, with seven different tools for extending those activities.

These STDCs provide the perfect starting point for discovering security threats that emerge as a consequence of the introduction of quantum technologies within the domain of computing. The following section discusses and engages in the *Multi-Dimensions of Threat Discovery* activity to determine the threats of these quantum technologies in computing.

Multi-Dimensions of Threat Discovery Using Security Threat Discovery Cards

The *Multi-Dimensions of Threat Discovery* (MDTD) activity aims at having participants consider a specific system. With that system in mind and using the entire card deck, participants explore card combinations from

[4] https://securitycards.cs.washington.edu/cards.html

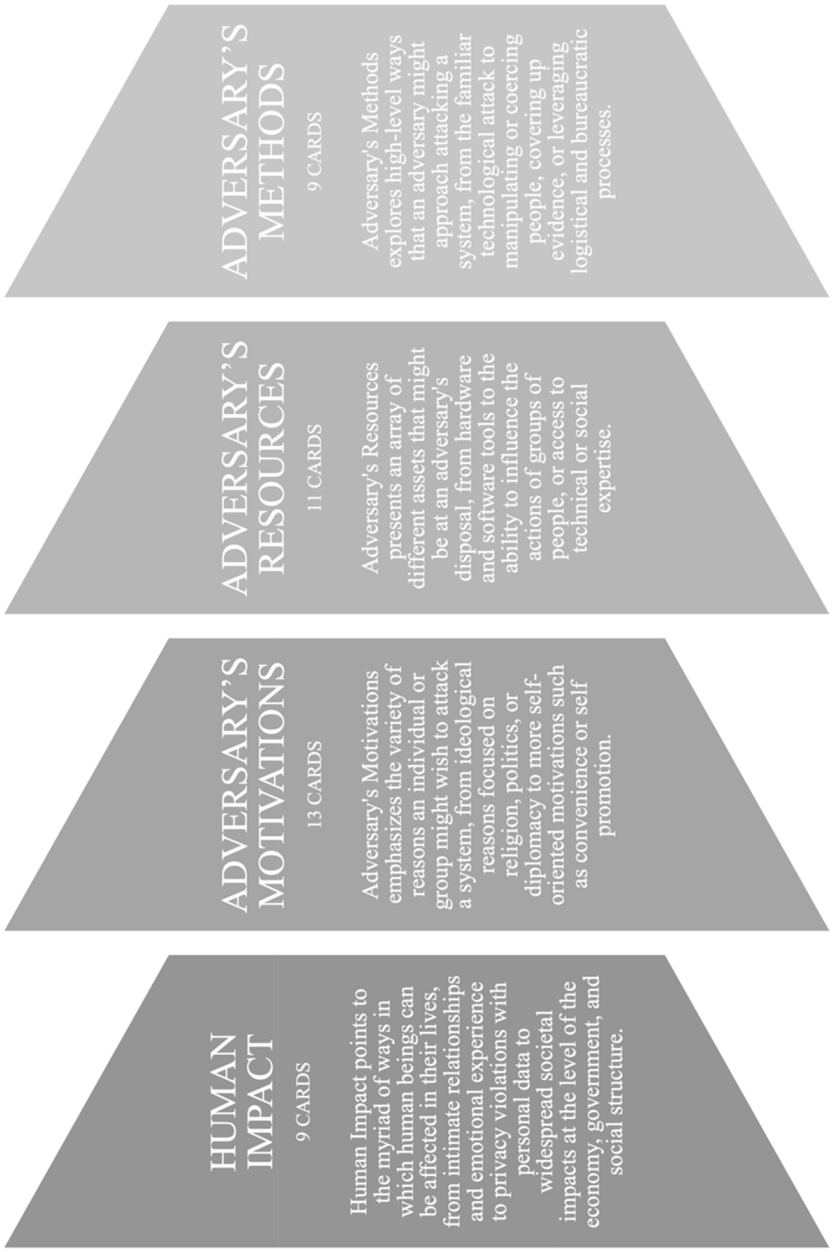

Fig. 2 Four Dimensions of the Security Threat Discovery Cards. Source: Denning et al. [3]

different dimensions to surface possible threats to the system. In doing so, they are encouraged to explore which combinations of cards surface critical threats, which combinations surface surprising threats, and which threats are most relevant overall. In completing the activity, participants should be able to identify (likely) direct and indirect stakeholders in the system, be able to argue how a compromised system might negatively impact direct or indirect stakeholders, and be able to identify at least 3 security threats that are relevant to the system.

Setup

A specific (hypothetical) system is presented to participants for analysis (i.e., a scenario). At this point, the system is merely described with no security analysis.

Break into groups

Participants are encouraged to work in collaborative groups of 4+ during which the research team functions in an observatory role. At this point, participants are asked to familiarize themselves with the card dimensions and the general format of the cards. Participants should read at least one card in each dimension in its entirety.

Threat Surfacing Activity

Identify Direct and Indirect Stakeholders (5 min) Participants are asked to sort the cards within each dimension in the order of relevance to the system under analysis.

Identify Human Impacts (7 min) Using cards in the Human Impact dimension, groups are asked to identify ways that the system could potentially be used or abused to impact direct and indirect stakeholders negatively.

Threat Surfacing Task: Multi-Dimension Combinations (10–15 min) Groups are given time to explore potential threats to the system, where a threat is defined as a potential action from an adversary. Groups are asked to consider a series of threats by (randomly or purposefully) selecting sets of cards; these sets should contain cards from at least two different dimensions (e.g., Adversary's Motivations and Adversary's Resources, or Adversary's Resources and Adversary's Methods). Groups are asked to discuss which 3 threats to the system are the most relevant to the system. Participants are informed that there is no "right" or "wrong" ordering. Participants may interpret "relevance" differently - for example, the realism of the attack attempt vs. the likelihood of attack success vs. the effect of a successful attack. The important aspect of 'relevance' is to be able to explore and articulate what makes the different threats more or less relevant.

Report Back

Participants are asked to present their identified stakeholders, the human impacts that might be impacted by system compromise, threats that they identified to the system, and the security and privacy risks with the chosen technology. Finally, participants are asked if any of the issues they identify are surprising to them.

Conceptual Investigation

In order to determine what (potentially) novel security issues may arise from quantum technologies, this paper presents a taxonomy of security issues as they are presented within the literature. The taxonomy (Fig. 3) is categorised both by type of quantum technology as well as the associated security risks split by domain, in this case: the issues particular to civil and defence domains. The taxonomy covers three broad quantum technologies: (1) quantum internet,[5] (2) quantum computing,[6] and (3) quantum sensing.

In order to determine the relevant security threats, both in civil and defence domains, concerning the realistic future application of quantum technologies, this paper employed the literature review approach proposed by Randolph [14].

[5] Quantum key Distribution (QKD) is already tested on quantum internet links, and possibly already operational; direct transmission of larger amounts of information is not realistic in the near future.

[6] Breaking standard encryption with quantum computers is possible if they can house millions of qubits, and that will take some time. There is doubt about whether quantum computing can be used for faster big data analysis because the speed up of quantum computing may be annulled by longer times to transform the data in quantum format.

Keywords

An iterative abductive process was necessary to identify relevant keywords. The process began with creating a *prima facie* list of potentially relevant keywords. Next, sources using those keywords were identified iteratively. Keywords were then modified based on the relevance of these sources. Sources that were too specific were reviewed in-depth for relevance, while overly general sources were reviewed based on sources that cited them. To ensure the quality and relevance of the selected literature, we selected 2 static keywords and 3 variable keywords that were used either independently or together in some combination (see Supplementary File 1).

Research Coverage

The coverage of this literature is an "exhaustive review with selective citation" (in [2] as cited by [14]. The aim was to formulate a comprehensive list of scholarly articles relevant to "security risks of quantum technologies." Given the relative novelty of the subject, there are a restricted number of available sources (i.e., [11, 16]). Many of the sources focused more on the technical aspects of these technologies, without an explicit or in-depth discussion of the relevant security issues involved. This review, rather, focuses on the broader security threats of quantum technologies that are explicitly mentioned in the existing literature.

Inclusion and Exclusion Criteria

Given the number of technical sources discussing these topics that may be of relevance, but only in an ancillary way. This paper narrows down the scope of inclusion to sources that best convey both the history and state of the art. It must also selectively exclude sources that may be redundant or less-than-relevant. The following list of criteria for inclusion/exclusion is informed by Randolph [14]:

1. Only English sources;
2. Only publications in academic journals, books, PhD theses, and reports from both government and NGO institutions;
3. Only sources from PhilPapers, the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), and Springer databases (excluding patents and citations).

Only sources that included "quantum computing", "quantum internet", "quantum sensing" AND "security risks" in the title, abstract, and/or as keywords.[7]

Overview of Final Sources

The review looks at the literature from January 1990 to December 2021. We identified 78 articles, books, theses, and reports in total. These sources are listed in Supplementary File 2. Figure 4 below illustrates the marked rise in the literature on quantum technologies with their related security issues spanning the search parameters.

These literature sources were processed using a proprietary natural language processing (NLP) system in order to summarize the literature for manual review. The NLP used performed two tasks with the literature 1) text summary and 2) topic extraction.

Text Summarisation

Text summarisation was performed starting from the upload on a Flask server (Python) of a document in PDF format from which only the textual content was considered, discarding any other media, such as images. A preprocessing phase was then carried out in which 'chunks' of 1000 tokens each were considered, meaning that sentences that did not exceed the maximum size that can be used by the transformer model used were excluded [17], see also [24].

Topic Extraction

Topic Extraction is carried out with an LDA (Latent Dirichlet Allocation) model, which is a generative statistical model particularly useful for extracting topics from a text (e.g., [9]. Also, in this case, there was a preprocessing phase in which words that were not considered useful (stop words), punctuation, and POS

[7] Boolean search strings using the keywords ensured fidelity in the results. Relevance weights of a value of '3' were used (the keyword must appear at least three times among the search domain parameters) to increase the probability of relevant results; see Supplementary File 1.

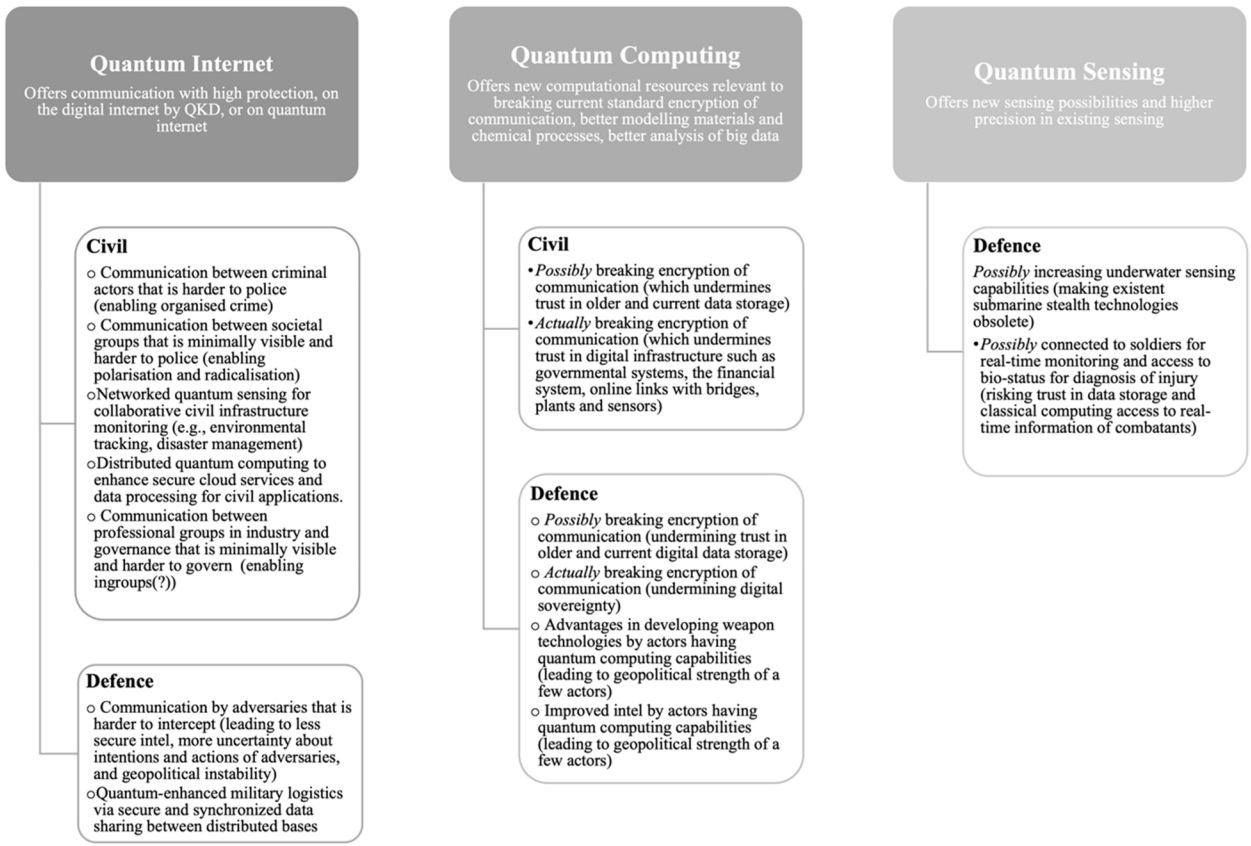

Fig. 3 A list of civil and defence security issues that emerge or increase by realistic future application of quantum technologies. (The security issues may be ones that did not yet exist and are specific to quantum technologies. and they may be ones that did exist but are substantially advanced by the emergence of quantum technologies. (Clearly there is in the latter case a problem of demarcation with determining whether an advance of a security issue is "substantial"). Civil applications of quantum sensing, such as the port security scenario presented in this paper, are less frequently discussed in the existing literature. Further exploration of potential civil uses is needed to fully capture the breadth of its applications)

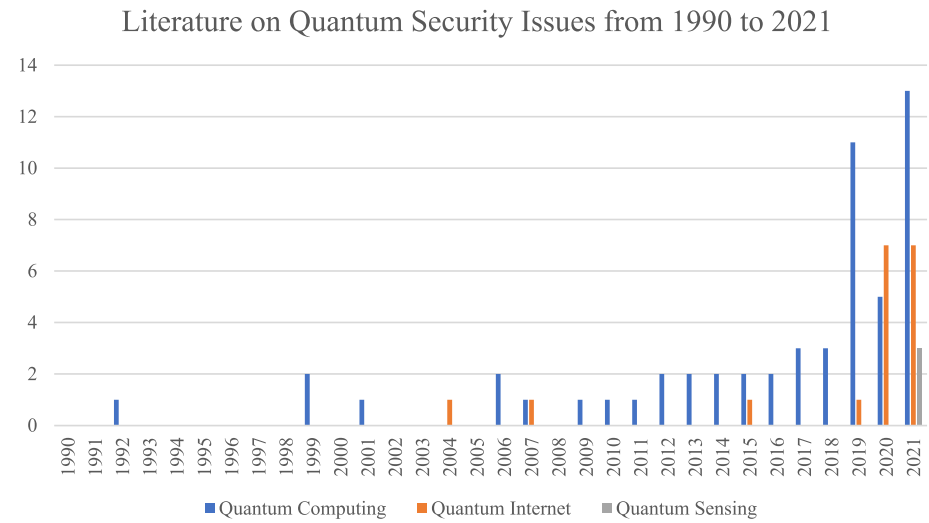

Fig. 4 Quantum Security issues Literature spanning 1990 to 2021

(Part Of Speech) of little relevance were removed from the source text, keeping only adverbs, nouns, verbs, and adjectives. Finally, the remaining words (the relevant ones) were lemmatized, i.e. the basic form is considered (Ex: ate -> eat). Finally, the set of lemmatized sentences was passed to the LDA model, which outputted a generation of topics (see Supplementary File 3). Each topic generated was characterized by a large number of words in order of significance.

While the conceptual investigation provided a structured understanding of the ethical, social, and governance challenges inherent in quantum sensing technologies, it is crucial to validate these concerns through empirical research. The application of STDCs within a real-world setting allows us to test whether these conceptual concerns are recognized by security practitioners and how they manifest in practical scenarios. This empirical investigation thus serves as a bridge, ensuring that theoretical concerns translate into actionable insights for organizations looking to integrate quantum sensing technologies.

Empirical Investigation of Security Risks in Quantum Sensing

Scenario Development

In an innovative approach to enhancing port security, a hypothetical scenario involving a Quantum Sensing System (QSS) was collaboratively developed by our research team. This process involved extensive research into current sensing methods used in ports and a forward-looking projection of how quantum sensing technologies might be integrated in similar contexts. The scenario was designed to reflect realistic near-future deployment possibilities, supported by a detailed graphic illustration (Supplementary File 4). The semi-structured expert interviews conducted in this study provided further validation of the scenario's plausibility, ensuring its alignment with practical considerations and technical feasibility. This scenario served as a structured basis for evaluating potential security risks and the applicability of Security Cards in a quantum technology environment.

Case Study Environment: the Port of Moerdijk

The Port of Moerdijk is the fourth seaport of national importance and the second container port in the Netherlands. It directly and indirectly employs more than 19,000 people. It has 5 harbor basins and is accessible via several highways connecting with the rest of Europe. The Port of Moerdijk has already employed smart technologies and data-driven solutions to enhance its operations, safety, and security. For example, all traffic and movements in the port are monitored using cameras and classical sensors to implement smart capabilities such as automatic license

plate registration, weighing of passing vehicles, and anomaly detection. Moreover, the Port of Moerdijk uses a cloud-based data management platform to collect data about its assets and plan their inspection and maintenance.

Scenario Description

The envisioned QSS at the Port of Moerdijk represents a breakthrough in maritime security, harnessing the principles of quantum mechanics. Positioned strategically along the canals, these advanced sensors form an invisible underwater security network, intricately woven throughout the port's expanse. The QSS operates by detecting objects within its range, and analyzing their composition from standard cargo to complex structures. It meticulously records the shapes of vessels below the waterline, discerns objects resting on the canal bed, and traces the movements of submerged entities like submarines, packages, and divers.

Furthermore, the QSS is evolving to penetrate vessels, identifying open spaces and analyzing materials within them. While these functionalities are still emerging and somewhat speculative, they point towards the future evolution of the QSS. The data collected by these sensors, represented as quantum bits, is securely transmitted via dedicated quantum lines to the port's control tower. Here, a sophisticated quantum computer processes this influx of information, performing rapid and complex computations to interpret the sensor data. This system, governed by the principles of quantum mechanics, ensures that only the output of the quantum computer is accessible, maintaining the integrity and confidentiality of data processing.

Objective

The development of this QSS scenario was strategically designed to serve two key purposes: Firstly, it provides a realistic and tangible context to identify potential security risks associated with advanced quantum sensing technologies. Secondly, it acts as a testing ground to evaluate the effectiveness of STDCs.[8] By simulating a plausible quantum sensing environment in a high-stakes setting like the Port of Moerdijk, we aim to assess whether the STDCs can effectively surface novel security risks that might not be immediately apparent through conventional analysis. This scenario, therefore, is instrumental in exploring the practical applications and limitations of STDCs in the emerging domain of quantum technology security.

Security Threat Discovery Cards Workshop with Port Personnel

Workshop Setup

The workshop titled "The Security Cards – Multi-Dimensions of Threat Discovery" was designed to unfold over a maximum duration of two hours. Its primary aim was to engage Port of Moerdijk personnel in identifying potential security threats associated with implementing a QSS using the STDCs. Eleven participants, including the Harbour Master, law enforcement officers, security coordinators, and security consultants to the Port, were invited by the Harbour Master to contribute their expertise.

The workshop began with presentations to familiarize participants with quantum technology, the specific application of this technology in the port scenario, the STDC tool, and the principles of value-sensitive design. Participants were then divided into two groups, each led by a moderator, to facilitate focused discussions.

The fourth and fifth authors of this paper assumed the moderator role. They had little to no prior knowledge about port security and were not informed about the use case scenario beforehand. This was intentional to avoid moderator bias and to simulate a realistic context in which an organization might deploy the STDCs with facilitators unfamiliar with the specific security domain. The moderators primarily coordinated MDTD activities, answered participant questions, and recorded observations throughout the session.

The workshop followed a structured format to ensure consistency in data collection. Participants engaged in open-ended discussions structured by the card categories, surfacing security risks based on their expertise and the fictional QSS scenario. Each group generated a written list of identified threats, supported by verbal discussions, while moderators took detailed field notes capturing observations and non-verbal cues (see Supplementary Files 2 and 4).

[8] See: https://securitycards.cs.washington.edu/

Data from the workshop consisted of: (1) participant-generated threat lists, (2) moderator field notes, and (3) observational accounts of group dynamics and interactions. These materials formed the basis for a manual thematic analysis. The analysis followed Braun and Clarke's [1] six-phase methodology: familiarization with the data, initial coding, searching for themes, reviewing themes, defining and naming themes, and producing the report. Three researchers independently reviewed the group outputs and notes to identify key categories of risk. Themes were then collaboratively discussed and refined through team deliberation, allowing for intersubjective agreement and triangulation between data sources. This approach enabled the identification of nuanced socio-technical, governance, and ethical risks beyond the surface-level content of the threat lists. No automated analysis software was used, as the goal was to maintain sensitivity to context and meaning embedded in the live workshop setting.

While qualitative software was not employed, the use of multiple data sources, comparative cross-group coding, and iterative discussion among researchers contributed to the rigor and transparency of the analysis.

MDTD Activity Description

Participants were tasked with a series of activities to surface potential security threats using the STDCs. Initially, they were presented with a system description sans security analysis to provoke unbiased consideration. Groups of three to four were then formed to discuss and familiarize themselves with the dimensions and formats of the STDCs.

The threat surfacing activity was structured into several steps:

1. Identification of direct and indirect stakeholders within the system.
2. Recognition of human assets at risk in case of system compromise.
3. Exploration of potential threats through various combinations of STDCs, with a mandate to identify and prioritize three threats deemed most relevant to the system.

Participants were encouraged to interpret "relevance" subjectively, considering factors like the realism of attack attempts, the likelihood of attack success, and the impact of successful attacks.

Workshop Findings

The workshop findings, derived from the participation of various stakeholders associated with the Port of Moerdijk, reveal a multifaceted perspective on the potential security threats posed by the integration of quantum sensing technologies. This section aims to provide a more comprehensive and nuanced account of these findings, enhancing the understanding of the complex security landscape that surrounds the deployment of such advanced technologies in critical infrastructure settings. Key threats identified by the groups included:

- *Curiosity-Driven Vulnerability Exploration:* This threat underscores the allure of new, advanced technologies to hackers, driven by curiosity or boredom, potentially leading to the discovery and exploitation of system vulnerabilities. This scenario emphasizes the need for continuous vulnerability assessment and threat modeling to anticipate and mitigate such risks.
- *Data ownership and management concerns*: Participants highlighted the criticality of data captured by quantum sensors, raising concerns over ownership, control, and the secure management of this data. The discussions pointed to the potential attractiveness of this data to various actors, including state and non-state entities with malicious intentions. This threat accentuates the importance of establishing clear data governance frameworks and implementing robust data protection mechanisms.
- *The human factor*: A significant concern raised was the potential for increased automation to erode interpersonal relationships and heighten dependency on technology. This scenario also painted a picture of potential internal resistance or rebellion, which could be exploited by external bad actors, such as drug dealers, aiming to corrupt employees. Notably, this threat is not purely speculative; employees have been made aware through existing campaigns of this vulnerability, reflecting an extrapolation from current, acknowledged issues with corruption and employee integrity. This insight calls for a balanced approach to automa-

tion, one that maintains human oversight and fosters a culture of security awareness and resilience.
- *Increased complexity of the overall system*: leading to heightened dependencies on a narrow group of experts. This complexity not only makes the system harder to understand and manage but also introduces risks related to the integrity and reliability of these experts. This concern was further elaborated with potential vulnerabilities, including hacking, abuse of power, and physical infrastructure attacks.

Additional Threats Identified

- *Inter-Port Competition*: A scenario where obsession and competition between ports, such as Amsterdam, Rotterdam, and Antwerp, could lead to a 'survival of the fittest' situation, potentially sidelining security considerations. It is important to highlight that this scenario envisages a 'race to the bottom', where ports might too hastily introduce and adopt quantum sensing technologies without proper due diligence, aiming to 'outsmart' their competition. This reckless pace could compromise not just the security but the integrity and reliability of the technologies employed, underscoring the need for a cautious and measured approach to technological advancements.
- *Over-Dependence on External Technologies*: Concerns were voiced about the dependency on technology providers, particularly from geopolitical rivals like the USA and China, which could introduce vulnerabilities and dependencies.
- *System Lock-In and Environmental Risks*: The potential for system lock-in, where the port becomes overly reliant on a single technology or vendor, and the risk of environmental incidents escalating due to over-dependence on sensor data, were also discussed.

The workshop highlighted the critical role of diverse stakeholder engagement in identifying and understanding the potential security threats associated with quantum sensing technologies. The rich dialogue underscored the importance of considering both technical and socio-technical dimensions of security, emphasizing the need for a holistic approach to safeguarding critical infrastructure. Furthermore, the findings illustrate the necessity of clear communication, stakeholder education, and the development of comprehensive security strategies that address the identified threats in a nuanced and proactive manner. These insights underscore the importance of a multidisciplinary approach to security, one that integrates technical safeguards with an understanding of human factors and organizational dynamics.

Semi-Structured Interviews with Security Experts

Methodology

For benchmarking the findings of the workshop, the study also employed semi-structured interviews to gather insights from experts in port security. The primary objective of these interviews was to form a baseline to assess the effectiveness of the STDC approach. The participants were selected based on their expertise in port security in relation to technologies and familiarity with ports on the North Sea coast, of which the Port of Moerdijk forms a part. They were unaware of the outcomes of the STDC workshop. The interviews were conducted on a secure online platform, ensuring good audio and video quality. Participants were given the QSS scenario in advance and informed that the sessions would be recorded for data accuracy. The interview guide comprised introductory remarks and a series of scenario-based, security, value, judgment, and open-ended exploration questions.

The semi-structured interviews were conducted using a standardized interview guide to maintain consistency across respondents. Each interview lasted between 45–60 minutes. The research team interviewer took detailed, non-verbatim notes. Manual thematic analysis was applied to the transcripts. Thematic analysis of the interview data followed a manual coding procedure informed by Braun and Clarke's [1] six-phase approach. Given the semi-structured nature of the interviews and the consistent format of questions, the research team conducted comparative coding across responses. Themes were identified through repeated readings of detailed interviewer notes, enabling cross-case comparison. Discussions among researchers ensured intersubjective agreement and minimized individual coder bias.

Findings

Experts provided varied perspectives on the QSS and its potential impact on port security. Key themes included:

Effectiveness and Futurism:

- *Expert 1's Perspective*: This expert lauds the QSS for its high effectiveness and views it as a beacon of futurism in security technology. However, the excitement is tempered by pragmatic concerns over the financial logistics and control mechanisms necessary for its implementation. This reflects a broader discourse in technological adoption, where the balance between innovation and practicality is often delicate and fraught with challenges.
- *Expert 3's Analysis*: Contrary to Expert 1, Expert 3 perceives the QSS as a logical extension of existing technologies, albeit with a critical eye on the intrinsic challenges of data interpretation and the assumptions underlying the models that power the system. This skepticism underscores a crucial aspect of technological evolution – the leap from theoretical innovation to practical application is often bridged by the robustness of underlying data and the interpretive frameworks that govern them.

Specificity and Human Factor:

- *Expert 2's Concerns*: The issue of specificity, especially in distinguishing between divers and dolphins, raises significant operational questions about the QSS. This concern is emblematic of broader challenges in security technologies, where the precision of threat detection must be balanced with the avoidance of false positives. Moreover, the emphasis on the human element as a potential weak link in security systems underscores a perennial truth in cybersecurity: technology can fortify defenses, but human behavior and integrity are often the linchpins of system vulnerability.

Ethical and Privacy Concerns:

- *Unified Expert Concerns*: All experts converge on the ethical and privacy implications of the QSS, a testament to the growing recognition of these issues in the deployment of advanced security systems. The ethical dilemma of scanning human bodies, as highlighted by Expert 2, touches on deep-seated concerns about bodily autonomy and the moral limits of surveillance. Meanwhile, Expert 3's insights into the implications of constant monitoring spotlight the trade-offs between security and privacy, a debate that is increasingly pertinent in an era where digital surveillance capabilities are expanding.

The analysis of expert opinions on the QSS reveals both excitement and caution. While the system promises a new frontier in port security through its advanced capabilities, it also raises fundamental questions about the balance between technological advancement and ethical governance. The concerns over specificity, human factors, and privacy underscore the need to approach security technology more broadly, and quantum technologies applied to the field more specifically, with a multifaceted perspective.

Analysis

The semi-structured expert interviews conducted to evaluate the QSS for the Port of Moerdijk provided insights into the complex interplay of technological innovation, security, and ethical considerations. Through detailed analysis of these interviews, it becomes evident that while the potential benefits of QSS are significant, they are accompanied by a nuanced set of concerns that warrant careful consideration. The interviews highlighted several common concerns among the experts:

- *Governance and Control*: Experts highlighted the critical issue of governance and control over the QSS, questioning who would hold authority over the system and its data. Expert 1 emphasized the importance of determining whether control should rest with the port authority, customs, or a combination thereof. The diversity of access and the necessity for role-congruent data usage were underscored, suggesting a layered approach to data access that aligns with the specific needs and responsibilities of various stakeholders. This perspective stresses the need for a clear governance framework that delineates authority, responsibility, and access rights within the QSS ecosystem.

- *Human Factor in Security*: The vulnerability of the QSS to human factors, such as corruption or hacking, was a concern shared across the interviews. Expert 2 pointed out that no matter the technological sophistication of the QSS, it cannot fully mitigate risks associated with human actors, particularly those in positions of trust or authority. This concern is rooted in the recognition that technology can serve as both a tool for security enhancement and a vector for exploitation, highlighting the enduring relevance of human integrity and vigilance in the security equation.
- *Privacy and Ethical Implications*: Significant privacy and ethical issues were raised, especially concerning the continuous and pervasive surveillance capabilities of the QSS. Experts grappled with the balance between enhanced security and the potential for invasive monitoring, which could lead to misuse of data or infringe upon individual rights. Expert 3's reflections on the analogy with current X-ray systems and the potential for implicit consent through port entry raise important considerations for legal and ethical frameworks governing such technologies.
- *Technology Limitations*: Concerns about the technological limitations of the QSS, particularly its vulnerability to hacking and the interpretive challenges posed by complex data, were noted. The reliance on assumptions and models for data interpretation underscores the need for transparency and critical evaluation of the underlying algorithms and decision-making processes. While quantum systems offer superior security features, such as quantum key distribution and quantum-enhanced cryptography, they also introduce new challenges, such as potential hardware vulnerabilities and the nascent state of integration with classical systems. As highlighted by Expert 3, these uncertainties necessitate ongoing research into robust security protocols and the development of quantum-resistant cryptographic methods to fully realize the security potential of quantum systems.

The expert interviews underscore the multifaceted challenges and considerations involved in implementing quantum sensing technologies in port security. They highlight the importance of addressing governance and control mechanisms, acknowledging the limitations of technology in mitigating human-centered risks, navigating privacy and ethical considerations, and confronting the technological vulnerabilities of quantum systems. These insights suggest a cautious yet optimistic approach to the adoption of QSS, emphasizing the need for comprehensive planning, stakeholder engagement, and continuous evaluation to balance the benefits against potential risks and ethical concerns.

Evaluation of Security Cards' Efficacy

Comparative Analysis

In qualitative research, we understand "validation" not in a statistical sense, but as a form of triangulation—the convergence of insights across independent data sources and methods that enhances the trustworthiness of findings. In this case, consistent themes such as governance concerns, vulnerability to human error or corruption, and data ethics arose across both methods, reinforcing their salience. However, the workshop also revealed risks less prominent in expert interviews, such as psychological responses to surveillance ("Big Brother" sentiment), institutional rivalry between ports, overdependence on foreign technology providers, and speculative threats like system lock-in and environmental vulnerabilities.

These divergences underscore the complementary strengths of the two approaches. While the expert interviews offered in-depth operational and technical reflections, the STDCs enabled broader socio-technical and organizational insights. Rather than using one method to "validate" the other, we argue that the overlap between them offers qualitative corroboration, while their differences enrich the total landscape of risks that stakeholders must consider.

Ultimately, the findings demonstrate the capacity of STDCs to engage non-expert stakeholders in rigorous and meaningful security assessments, while also surfacing concerns that might be overlooked in more traditional expert-based analyses. This strengthens the case for using participatory tools like STDCs in early-stage risk governance for emerging technologies like quantum sensing.

Effectiveness Analysis

The STDCs have proven effective in drawing out a diverse array of potential security risks that extend beyond the immediate technical and operational concerns of the quantum sensing system. The structured format of the cards, which encourages participants to consider multi-dimensional threat scenarios, contributed to identifying risks related to socio-technical systems and broader societal impacts. Participants in the workshop, a mix of individuals with various roles in port security, were able to identify threats that may not be immediately evident to security experts. This implies that the STDCs can be a valuable tool for collaborative risk assessment, bringing together multiple perspectives and expertise areas to anticipate a wider range of potential security issues.

The efficacy of the STDCs in this context suggests that they can be a significant addition to traditional risk analysis methods in the realm of advanced quantum sensing technologies. Their ability to facilitate the identification of non-obvious, emergent risks is particularly relevant given the complexity and novelty of quantum technologies, where established risk assessment frameworks may fall short. However, the effectiveness of the STDCs also relies heavily on the participants' engagement and the facilitators' ability to guide the discussion. The diverse backgrounds of the workshop participants suggest that the STDCs can help bridge gaps in understanding and foster a comprehensive security culture among various stakeholders.

Beyond confirming that STDCs are effective tools for identifying security risks in quantum sensing applications, this study highlights potential ways to refine and extend their use. One key insight is the importance of tailoring STDCs to domain-specific threats. In the case of quantum sensing, future iterations of the cards could include categories explicitly addressing quantum-specific adversarial scenarios, such as quantum-enabled cyberattacks, sensor spoofing, or privacy breaches from quantum-enhanced surveillance. Moreover, this study suggests that STDCs can be a foundational tool for broader risk governance in emerging quantum technologies. As quantum computing, quantum cryptography, and quantum sensing develop, there is a need for proactive methodologies that do not rely on retrospective risk assessments but instead enable stakeholders to anticipate and shape technological trajectories. This positions STDCs not merely as a tool for security threat discovery, but as a participatory design instrument that fosters responsible futuring of quantum technologies. By embedding STDCs within value-sensitive design processes, organizations could iteratively refine their risk assessment frameworks to account for both technical vulnerabilities and broader societal impacts. This approach would align with the anticipatory ethics movement, helping stakeholders move beyond merely responding to risks and instead proactively shaping responsible quantum innovation.

Limitations and Recommendations

The study's limitations include potential biases in the selection of the experts, of the Port of Moerdijk, and in the selection of the participants to the workshops. For instance, all participants were related to the Port of Moerdijk and may share certain institutional perspectives. Moreover, the complexity of the STDCs' English terminology posed a language barrier in the workshop, since all participants were native Dutch speakers and not familiar with the academic English terminology used in the texts on the STDCs.

Future research should explore the application of STDCs across different industrial and technological contexts and global cultures to validate their universal applicability. Additionally, further development of the cards to include localized language options and context-specific adaptations could enhance their usability and effectiveness.

Conclusion

This paper has demonstrated the potential of Security Threat Discovery Cards (STDCs) as an effective tool for identifying security risks in emerging quantum sensing technologies within port security contexts. Through a workshop with Port of Moerdijk personnel and interviews with security experts, it was shown that STDCs can help uncover nuanced risks that might not be immediately apparent, such as socio-technical threats and broader societal impacts. In the introduction of this paper, we identify two challenges to such risk analysis: that applications of quantum technologies are not yet well-developed, and that quantum technologies are often perceived as incomprehensible,

making stakeholders shy away from analyzing applications. Our findings suggest that both challenges can be overcome: organizations and companies considering the integration of quantum technologies can utilize STDCs to independently identify significant security risks early in the technology development and implementation phases without being hampered by the quantum nature of these technologies.

The comparative analysis of the findings from both studies highlights the STDCs' capability to reveal risks beyond the foresight of experts, particularly when applied in a real-world context with direct stakeholders.[9] This indicates that STDCs can play a crucial role in proactive risk analysis of emerging technologies, enabling stakeholders to develop comprehensive security strategies that address known and emergent threats. In conclusion, the study affirms the efficacy of STDCs in facilitating a nuanced and comprehensive understanding of security risks associated with quantum sensing technologies. By empowering organizations to engage in self-guided risk assessments, STDCs provide a valuable tool for ensuring the safe and responsible integration of quantum technologies. Further research should explore the broader applicability of STDCs in other domains and refine the tool to enhance its effectiveness across diverse industrial and cultural contexts.

Acknowledgements All remaining errors are the authors' alone. First of all, we would like to thank Gijs-Jan Schüssler, the Harbour Master of the Port of Moerdijk, for his help in setting up and hosting the workshop. We want to thank Marco Bernardi for creating the proprietary NLP software used for text summarization and topic extraction. We would also like to thank the participants of the workshop, Jan Otten, as well as the three port security experts: Yarin Eski, Thierry Vanelslander, and Rob Zuidwijk, who served as the experts of the semi-structured interviews.

Author contributions All authors contributed equally to the ideation, writing, and editing of the manuscript.

Data availability All data are supplied as supplementary materials. Boolean search strings are available as supplementary file 1: Boolean search strings. Literature on security issues for quantum technologies is available as supplementary file 2: Quantum Security Issues. LDA model generated content can be found in supplementary file 3: LDA Model Content. The precise content of the scenario is available as supplementary file 4: Scenario.

[9] While not statistically validated, the convergence of themes between expert interviews and workshop participants provides qualitative triangulation, enhancing the soundness and robustness of the identified risks. Moreover, differences in findings highlight the complementary perspectives each method brings.

Declarations

Ethics approval and consent to participate This study was approved by the Ethical Committee of TU Delft (number 2246). All participants provided written informed consent. All research and work was performed in accordance with the relevant guidelines and regulations. We adhered to the Consolidated criteria for reporting qualitative research (COREQ) regulations throughout the process.

Consent for publication The undersigned authors affirm that all individuals who have contributed significantly to the writing and content of this article, including workshop participants and port security experts, have provided their consent for the publication of the material presented herein. This consent has been obtained in either written or oral forms, adhering to the ethical standards of academic integrity and research transparency. Each contributor recognizes and agrees to the publication of this work, understanding the implications and reach of its dissemination in the academic community and beyond.

Competing interests None of the authors has competing interests with regard to the content of this publication. The Authors, therefore, declare no competing financial or non-financial interests.

References

1. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qual Res Psychol 3(2):77–101. https://doi.org/10.1191/1478088706qp063oa

2. Cooper HM (1988) Organizing knowledge syntheses: A taxonomy of literature reviews. Knowl Soc 1:104. https://doi.org/10.1007/BF03177550
3. Denning T, Friedman B, Kohno T (2019) Security threat discovery cards [Ebook]. University of Washington. Retrieved 7 February 2022, from http://securitycards.cs.washington.edu/index.html
4. Dowling JP, Milburn GJ (2003) Quantum technology: The second quantum revolution. Philos Trans A Math Phys Eng Sci 361(1809):1655–1674. https://doi.org/10.1098/rsta.2003.1227
5. Flanagan M, Nissenbaum H (2014) Values at play in digital games. MIT Press, Cambridge
6. Friedman B, Hendry DG (2019) Value sensitive design: Shaping technology with moral imagination. MIT Press, Cambridge
7. Friedman B, Kahn PH, Borning A, Huldtgren A (2013) Value sensitive design and information systems. In Early engagement and new technologies: Opening up the laboratory (pp. 55-95). Springer, Dordrecht. https://doi.org/10.1007/978-94-007-7844-3_4
8. Gibney E (2019) The quantum gold rush. Nature 574(7776):22–24. https://doi.org/10.1038/d41586-019-02935-4
9. Gross A, Murthy D (2014) Modeling virtual organizations with Latent Dirichlet Allocation: A case for natural language processing. Neural Netw 58:38–49. https://doi.org/10.1016/j.neunet.2014.05.008
10. Han JW, Moon DI, Meyyappan M (2017) Nanoscale vacuum channel transistor. Nano Lett 17(4):2146–2151. https://doi.org/10.1021/acs.nanolett.6b04363
11. Krelina M (2023) The prospect of quantum technologies in space for defence and security. Space Policy 65:101563. https://doi.org/10.1016/j.spacepol.2023.101563
12. Kung J, Fancy M (2021) A quantum revolution: Report on global policies for quantum technology. CIFAR, Toronto. https://cifar.ca/cifarnews/2021/04/07/a-quantum-revolution-report-on-global-policies-for-quantum-technology/
13. Mikami K (2015) State-supported science and imaginary lock-in: The case of regenerative medicine in Japan. Sci Cult 24(2):183–204. https://doi.org/10.1080/09505431.2014.945410
14. Randolph J (2009) A guide to writing the dissertation literature review. Pract Assess Res Eval 14:13. https://doi.org/10.7275/b0az-8t74
15. Roberson T (2023) Talking about responsible quantum: "Awareness is the absolute minimum that… we need to do." NanoEthics 17(1):2. https://doi.org/10.1007/s11569-023-00437-2
16. Sonko S, Ibekwe KI, Ilojianya VI, Etukudoh EA, Fabuyide A (2024) Quantum cryptography and US digital security: A comprehensive review: INvestigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Comput Sci IT Res J 5(2):390–414. https://doi.org/10.51594/csitrj.v5i2.790
17. Sshleifer (2021) sshleifer/distilbart-cnn-6-6 · Hugging face. Huggingface.co. Retrieved 10 March 2022, from https://huggingface.co/sshleifer/distilbart-cnn-6-6
18. Schreck F, Druten KV (2021) Laser cooling for quantum gases. Nat Phys 17(12):1296–1304. https://doi.org/10.1038/s41567-021-01379-w
19. Temkin M (2021) VCs make record bets on quantum computing. Pitchbook.com. Retrieved 9 February 2022, from https://pitchbook.com/news/articles/quantum-computing-venture-capital-funding
20. Umbrello S (2020) meaningful human control over smart home systems. Humana Mente J Philos Stud 13(37):40–65
21. Umbrello S, Seskir ZC, Vermaas PE (2024) Communities of quantum technologies: Stakeholder identification, legitimation, and interaction. Int J Quant Inf 1-25. https://doi.org/10.1142/S0219749924500126
22. van den Hoven MJ, Vermaas PE, van de Poel IR (2015) Design for values: An introduction. In: van den Hoven J, Vermaas PE, van de Poel I (eds) Handbook of ethics, values, and technological design: Sources, theory, values and application domains. Springer, Dordrecht, pp 1–7. https://doi.org/10.1007/978-94-007-6970-0_1
23. Vermaas PE (2017) The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. Ethics Inf Technol 19:241–246
24. Wolf T, Debut L, Sanh V, Chaumond J, Delangue C, Moi A, …, Rush AM (2020) Transformers: State-of-the-art natural language processing. In Proceedings of the 2020 conference on empirical methods in natural language processing: system demonstrations (pp 38-45). Online. Association for Computational Linguistics. https://doi.org/10.18653/v1/2020.emnlp-demos.6
25. World Economic Forum (2022) (rep.). Quantum computing governance principles. Cologny: World Economic Forum. Retrieved February 7, 2022, from https://www.weforum.org/reports/quantum-computing-governance-principles