

Extended Reality in critical sectors: Exploring the use cases and challenges

Camille Sivellev, David Palma, and Katrien De Moor

NTNU – Norwegian University of Science and Technology, Department of Information Security and Communication Technology, 7034 Trondheim, Norway
`{name.surname}@ntnu.no`

Abstract. Critical sectors such as healthcare, energy production or defense increasingly consider the use of Extended Reality (XR) technologies as a way to enhance training and facilitate operations. In this context, immersive technologies bring forth new opportunities, but also a range of privacy and security challenges that, to date, remain understudied. To evaluate and address those challenges, there is a need to better understand the contexts and purposes for which XR is used in critical sectors. Based on data collected through an online questionnaire (N=6) and a series of semi-structured in-depth interviews (N=7) with professionals from a diverse pool of Norwegian organizations using XR, this study explores various characteristics of relevant use cases of XR, with a focus on critical sectors. Our findings indicate that XR, and in particular VR, is already used in a large range of sectors, with training being the most prominent purpose. Nonetheless, these use cases are still relatively immature and various barriers limit the current use of XR in critical sectors. Further, while privacy and security are considered to be important, they are not a driving concern yet, and will need to be further taken into account before XR can be leveraged more broadly in critical sectors. These results aim to help to orient future research efforts towards reconciling usability, security and privacy for XR in the Norwegian ecosystem.

Keywords: Virtual reality · Augmented Reality · Security · Privacy · Critical sectors

1 Introduction

Extended Reality (XR) is increasingly used in a variety of sectors such as industry, entertainment, culture. This term includes immersive technologies blending physical and digital elements into one environment — for instance virtual (VR), augmented (AR) or mixed reality (MR). Such technologies can be leveraged to enhance training, facilitate visualization and augment operations. In that regard, XR solutions are also starting to be applied in the context of critical sectors such as healthcare, energy production or emergency services.

Critical sectors are at higher risk of being targeted by cyber-attacks and data breaches [6], and XR brings many challenges in security and privacy that remain under-addressed in the literature [8, 18]. While already problematic in most use

cases, cyber-threats targeting XR technology are to be taken even more seriously in the context of critical sectors. For instance, spatial privacy risks in MR could lead to an attacker gaining access to sensitive 3D data [7], for example about the industrial environment it is used in. Researchers also showed that perceptual manipulations, for example redirected walking, could be exploited to lead to physical harm and safety risks [23] which could be particularly problematic for an operator using a Virtual Reality (VR) headset in an industrial environment. Finally, the extensive data collection performed by such devices (including eye tracking or body movement data) is particularly concerning in medical contexts [19], increasing the risk and impact of data leaks.

In order to better account for security and privacy challenges raised by immersive technologies, providing security features that are suited for XR represents an emerging topic, with the conceptualisation and evaluation of solutions such as authentication [11], intrusion detection [24] or privacy-enhancing features [16]. However, the threat scope of XR solutions is multi-layered, encompassing technological, societal and regulatory aspects [8]. This requires appropriate frameworks to address all the dimensions present in critical sectors.

While there is a growing body of literature and research on emerging use cases and innovative applications of XR, these technologies are also increasingly used by companies and other organizations outside of academia. However, there is an overall lack of systematized information about how it is actually used in different organizations, for which use cases and purposes, at which levels of maturity and with which results. Moreover, while security challenges raised by the adoption of XR [18] are often mentioned in the literature, it is still unclear how security is actually accounted for in organizations [2], notably by those in critical sectors.

The lack of a clear understanding of the actual XR use cases outside of academia is an issue, because the context of use also impacts the accuracy and usability of a given security solution. For instance, using behavioral biometrics (e.g., eye tracking patterns, head movements) has emerged as a way to authenticate people in VR. Previous works on that topic identify people based on their behavior during stationary, non-interactive experiences [13]. But when identifying participants based on the data collected from a VR training session, for example for troubleshooting a surgical robot in a robotic operating room, Moore *et al.* [14] report a noticeably lower identification accuracy compared to the results obtained in a previous study identifying participants observing 360-degrees videos. Therefore, to tailor solutions that are suited to XR in critical sectors, it is necessary to understand the relevant contexts of use, a fundamental step in the human-centered design process and in usability studies [12].

This study aims to fill the gap between XR technologies, security and privacy by conducting a first exploration of different use cases for XR in Norway, in particular in critical sectors. For this purpose, we adopted an exploratory research design combining an online questionnaire (N=6) and semi-structured interviews (N=7). Overall, this work aims to help identify pressing research directions and study solutions that are adapted to the most relevant issues and gaps in the XR landscape in Norwegian organizations. To the best of our knowledge, this study

is the first attempt to propose a mapping of the XR use cases in Norway that accounts both for social and technical aspects. Moreover, the presented study is not limited to secondary data sources, but instead draws on an online questionnaire and semi-structured interviews to collect the insights of the stakeholders involved in the various XR use cases that exist in industry and other institutions. More concretely, we address the following research questions:

- **RQ1:** What are the existing contexts in which XR is developed and used in Norwegian organizations and what are their characteristics?
- **RQ2:** what are the challenges raised concerning the adoption of XR in critical sectors, notably in security and privacy?

In Section 2 we briefly introduce the main concepts and related work, followed by our methodology in Section 3. We describe our findings in Section 4 and discuss them in light of the literature, concluding with perspectives for future research in human-centered security and privacy for XR in Section 5.

2 Background

In the following section we provide some background information regarding the use of Extended Reality (XR) in critical sectors, then we introduce the central notion of context of use and position this study with regard to the literature.

2.1 Extended Reality in Critical Sectors

A growing body of research focuses on new ways to use XR in so-called “critical sectors”. Because XR allows for better engagement and improved learning capacities, it is relevant for training in several professions in critical sectors (e.g., emergency workers or operators working in hazardous environments such as mines) [1]. The European Commission defines critical entities as “*providers of essential services, [which] play an indispensable role in the maintenance of vital societal functions or economic activities*” [22]. A critical sector is an industry sector that contains such entities. The associated directive provides a list of critical sectors which includes energy, transport, banking, health, water, digital infrastructures, public administration, space or food.

In some critical sectors, training in “real” conditions is impossible, can pose safety or ethical issues, or has too high a financial cost. XR training can address these challenges and enhance learning engagement [20]. XR use cases in critical sectors are not limited to training but also extend to other purposes, for example to allow for remote collaboration in shipyard pipe workshops, to carry on research experiments at a lower cost, or to help complex model visualization [1]. From these different examples it is already clear that both the context, but also human and system-related factors may differ greatly from one use case (and associated objective or purpose) to another. There is consequently a need to carefully explore and investigate them.

2.2 Context of use in human-centered design

In order to accurately evaluate the usability, efficiency or security of an XR solution, having access to representative users and context is a necessity [21]. Usability and human-centered design (HCD) standards rely on the notion of context of use [9, 5], which consists of “*the goals of the user community, and the main user, task and environmental characteristics of the situation in which it will be operated*” [12, p. 1]. The ISO 13407 standard [9] on HCD includes the analysis of the context of use as one of the main stages of the HCD cycle. Further, Maguire [12] provides a description of the main contextual factors: user, tasks and environment, itself divided in technical, physical and organizational aspects.

A few works applied context of use to XR. For instance Cramer *et al.* [4] applied contextual analysis on a VR radiology explorer system, and VanWyk *et al.* [25] on a VR application for safety training of miners. However, both focused on usability aspects without accounting for the potential impacts on security and privacy. In addition, and to the best of our knowledge, no prior studies focused explicitly on the XR landscape in critical sectors. In that sense, and drawing on the factors identified in [12], this study is the first to look at context of use components for XR in critical sectors with a focus on security and privacy.

Other research works mapped XR applications for specific sectors, for example exergames (health / entertainment) [10], or education [3]. Unlike this study, their findings are solely based on the secondary data sources (mostly the scientific literature, although Cradit *et al.* [15] relied on patents databases), and they do not account for the perspectives of the stakeholders involved in the XR use cases from the industry and other institutions.

3 Methods

In order to explore different XR use cases in Norwegian organizations and understand the associated security and privacy issues, we conducted an exploratory study, relying on a qualitative research design. The overall goal is not to quantify or be exhaustive, but rather to explore and bring attention existing challenges in this ecosystem. With respect to the research questions highlighted in Section 1, this study aims to (1) understand some of the various purposes for which XR is used in Norway, as well as their broader context of use, and (2) to get preliminary insights on the way security and privacy are handled and considered for these use cases. To this end, the adopted research design relied on both an online questionnaire and a series of in-depth interviews. We chose to offer the possibility to participate through either interview or filling the questionnaire in order to maximize participation and facilitate flexibility for respondents. Therefore, the themes and concrete topics covered in both data collection approaches of the study were following the same general structure.

Broad theme	Subtopics
Organizational context	Interviewee role, type, size, aim of organization Use of XR, Project maturity / technological readiness level
Tasks	Purpose of XR, use cases description, frequency of use
Technical environment	Used hardware and software
Target users	Role and characteristics
security and privacy	Regulations, compliance Existing features, steps taken to assess/improve security or privacy Needs and barriers
General challenges	Acceptance, funding Barriers and perspectives for broader adoption

Table 1. Questionnaire design

3.1 Data collection: online questionnaire and semi-structured interviews

The **online questionnaire** was divided in several parts, covering the motivation for using XR, sectors covered by XR-related projects, as several aspects for the different factors impacting the context of use. A second part focused more in-depth on specific projects and on perceived challenges and perceptions about security and privacy, and specific risks in regards with the use case. Table 1 provides an overview of the themes covered in the questionnaire. The questionnaire was pretested ahead of release and was administered in Nettskjema [17].

The **semi-structured interviews** used an interview guide aligned with the structure and thematic areas covered in the questionnaire, but offered more room for elaboration and to talk about multiple example projects. The interviews were conducted via Microsoft Teams and lasted approximately 1 hour each. 6 of the interviews were conducted by 1 main interviewer and 1 secondary interviewer and note taker. 1 of the interviews was conducted by the main interviewer alone.

A **targeted sampling approach** was used to reach out to professionals from both the private and public sector working with XR. We used searches from publicly available information (e.g., company websites, articles) to reach out to the targeted organizations. We also relied on relevant networks relating to immersive technologies (e.g., XR Norge [26]) as recruitment channels, in addition to a snowball-sampling approach via personal networks. The final sample (see Section 4) consists of respondents with different profiles and roles, both technical and non-technical, within the respective organizations, providing a broader overview of the contexts of use of XR and related challenges.

3.2 Data analysis and data protection

The data collection took place between August and September 2024. In total, 7 semi-structured interviews were conducted. Based on written consent of the interviewees, all sessions were recorded, transcribed and deductively coded with the main themes being directly derived from the interview guide and questionnaire. 6 additional participants representing different organizations responded to the questionnaire. Both parts of the study were reported to the Norwegian Agency for Shared Services in Education and Research and all data was gathered and processed in compliance with the legal frameworks for personal data.

Id	Role in the organization	Type of organization	Sectors	Focused Data from on XR	
P1	CCO	Private	Transportation	Yes	Questionnaire
P2	Researcher	Public	Misc.	No	Questionnaire
P3	Developer	Public	Health, transportation	No	Questionnaire
P4	Director	Private	Misc.	Yes	Questionnaire
P5	Researcher	Research	Misc.	No	Questionnaire
P6	CTO	Private	Misc.	Yes	Questionnaire
P7	CTO	Private	Healthcare	Yes	Interview
P8	CTO	Private	Misc.	Yes	Interview
P9	Lead developer	Private	Misc.	No	Interview
P10	Researcher	Public	Defense	No	Interview
P11	Researcher	Research	Healthcare	No	Interview
P12	Lead developer	Private	Energy	No	Interview
P13	CEO	Private	Misc.	Yes	Interview

Table 2. An overview of the participants (N=13), including their role, organization, sector where XR is applied, whether the organization focuses solely on XR or not, and whether the participant took part in the questionnaire (N=6) or in an interview (N=7).

4 Results

To present our findings we first provide an initial overview of the organizational contexts in which XR is used. We then detail some use cases regarding aspects such as: purpose and targeted user groups, scale and maturity level, technical context and sectors. Finally, we describe the a number of identified challenges associated with XR, as well as security and privacy concerns and practices highlighted by the participants.

4.1 Participants and organizational context

In total, the study involved 13 participants representing a variety of Norwegian organizations of varying sizes (from SME’s to large organizations with over 500 employees), including 8 private companies, 2 different research institutions and 3 governmental institutions (including a large municipality in Norway). They participated in the study because they either develop, commercialize and/or use XR in various sectors. Table 2 provides an overview of the participants, the types of organizations and sectors they work in. It shows that 8 of the participants have leading roles within their organizations (CTO, CEO, CCO, director, Lead developer), while the others are actively involved in XR research or development.

4.2 Use of XR in general

Use of XR. When asked in which way(s) the organization uses XR technology, a wide range of uses was reported (see Figure 1, the majority being active in development of XR software/applications (92%), researching new use cases

and applications for XR (46%), using XR without developing it (8%) and performance evaluation and measurement of XR (31%). None of the organizations focus on the development of XR hardware.

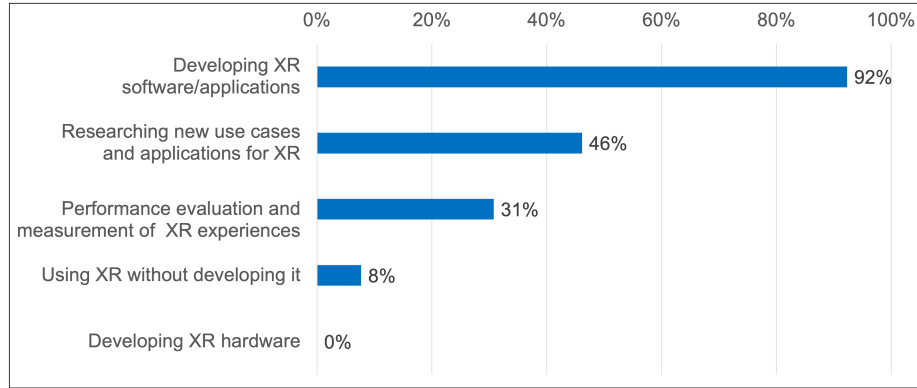


Fig. 1. Use of XR technology in the participating organizations.

Volume of XR projects. All participants but 3 reported that their organization is engaged with more than 1 project related to XR. In 5 cases, the reported projects within the same organizations are fully independent of each other and have a different purpose. However, another 5 respondents reported that their organization has several projects which are connected in some way, for example applications with similar purposes in the same sector. 3 of the involved organizations have developed or are developing a platform which can host different XR applications, sometimes targeting entirely different user groups. P8's company provides a platform with various training modules in distinct sectors — for example forestry or healthcare.

Application sectors. Interestingly, despite the limited sample, the participating organizations have projects relating to a wide range of application sectors, including transportation, telecommunications, energy, defense, healthcare, space, the maritime sector, education, culture, entertainment, marketing and design, emergency services or governmental services. For instance, P7's company specializes in the use of XR in the healthcare sector; P1 referred primarily to the transportation sector; and P12's organization focuses on the use of XR in the energy sector. On the other hand, P8, P9 and P13 work in companies that target a broader set of sectors (e.g., emergency services, energy, space, fishery).

Type of XR technology used. Virtual reality is used the most (10 of the participants' organizations use it in one or more projects), and most of the VR projects rely on VR headsets and standard controllers. In 6 of the organizations, there are also efforts involving mixed or augmented reality.

Organizational context. The organizational context behind the reported XR projects is rather diverse: Out of the 13 organizations involved in our study, 7 were small companies (5 to 50 employees) focusing on Extended Reality or (less often) on 3D development in general. However, there were also 6 bigger

organizations such as research institutions or large companies (500+ employees) with a totally different scope. In those organizations, smaller units work on XR as experienced by P12: *“I feel like a person with a little start up in a big company”*.

Temporal context. In all of the organizations encountered, the use of XR is still relatively recent (with some exceptions of companies such as P9, which was active in the area of digital design and visualization before focusing on XR). P10 noted that in general, the use of XR in Norway is still exploratory and relatively immature, and constituted of single projects mostly in a R&D phase.

4.3 In-depth use cases

Example projects. While interviewees were able to cover several projects, questionnaire respondents were asked to elaborate in-depth on one specific project. Use cases mentioned in the questionnaire include for example a sector-independent AR-enhanced training platform (P4), using XR for digital twins to simulate mitigation strategies and raise awareness around climate change (P5), using VR and AR for discussion exercises offering the possibility to place objects on a 3D map in the context of provision of emergency services (P6), or using XR to ensure compliance with infrastructural regulations (e.g., in relation to public roads, P1). In the interviews, a wide range of examples was given, from using VR to support children and adolescents diagnosed with autism spectrum disorder (P11), a VR (multiplayer) clean-up training after an oil leak (P9), a VR-based distributed, tactical operation center (in collaboration with NATO)(P8), using MR for planning and remote inspection of assets and installations (P12), or a VR-based course in strategical training for civilian protection (P10).

Purpose of using XR. The majority (at least 8 out of 13) of the organizations we studied were using XR for purposes relating to the training of their (or their clients’) personnel. For instance, P7 mentioned a project focused on the use of VR for training medical personnel in the primary healthcare sector. Similarly, other examples were given such as learning a procedure, extinguishing a fire in a tunnel or training to operate certain equipment (P8). However, P8 also referred to training scenarios that are more geared towards dealing with chaotic or uncertain situations (e.g., multi-stakeholder crisis management in the case of a crisis situation). Other purposes mentioned include data visualization, such as visualizing the layout of a plant (P12), recreating photo-realistic environments based on real locations (P6), or with the goal of helping in planning (e.g., maintenance operations or other interventions). Others used XR for remote assistance, e.g., in the context of remote inspection (P12), or infrastructural work (P1, P9).

Project scale and level of maturity. The majority of the reported projects are currently on-going (5 out of 6 in the questionnaire, and the most of projects described in the interviews), however, the number of people involved, as well as the reported maturity level vary greatly. Most of the projects (4 out of 6 in the questionnaire) consist of relatively small project teams (up to 9 people), with one exception (over 100 people involved). Similarly, the interviews indicated large differences: while some projects are rolled out and in use on a regular basis (e.g., training of medical personnel in different municipalities (P7), minority language

classes in VR (P8)), other projects are smaller in scale and focus on early stage testing of different solutions in terms of “*whether they are usable, rather than on perfection*” (P12). While several (e.g., P6, P11) projects have been validated in some scale (e.g., experimental proof of concept, validated in a lab setting or in the relevant environment), only a few projects resulted in a deployed system being used in operations in everyday life (e.g., P5, P7).

Collaborations and partnerships. In the questionnaire, all respondents but one reported collaborations with both academic institutions, as well as with other partners, such as municipalities, private companies with experience relevant to XR or the specific use case (e.g., fire prevention, automotive industry, municipalities). The interviewees, in particular those working for XR companies, also reported collaborations with different stakeholders (e.g., other companies/clients, academia, public authorities, the Norwegian armed forces). However, sector representatives such as P12, reported mostly in-house collaborations.

Application sectors. Despite the relatively small sample size, the reported specific projects cover a wide range of sectors. The transportation sector was most prominent in the questionnaire, followed by education, governmental services, emergency services, energy, health and telecommunications. One project is environment-oriented and one is sector-independent. Similarly, the use cases discussed in the interviews cover a wide range of sectors, with a clear tendency for most XR companies (except for P7) to be active in different sectors.

Targeted user groups. Along with the general variety in the reported projects, there is diversity in terms of envisioned user groups of the XR applications. However, employees (of various types, e.g., healthcare staff) represent a dominant user group. Only one of the reported projects targets regular consumers. Three organisations had projects targeting students, including language (P8) and military (P10) students, and pupils/students with special needs (P11).

Technological context. The questionnaire responses indicate a broad variety of hardware being used, ranging from AR glasses, wireless and cabled Head-Mounted Displays (HMDs), controllers, motion trackers, sensors, tablets, and browser-based VR in Personal Computers (PCs). The 6 AR/MR experiences also relied on software mostly developed by the organizations themselves (only one reported to additionally use some third-party software), and a combination of mobile, tablet and PC AR. P10 also reported on the use of artificial intelligence in a VR experiences in their organization. This allowed them to have more variation in the scenarios and to increase user agency. Interestingly none of the respondents reported on the use of other haptic feedback devices such as gloves. Price might be an important factor here: “*We have looked into gloves and like haptic suits (...) But currently it’s too expensive for the clients*” (P8). Some of the projects used a specific model of HMDs (Meta Quest 3 and Apple Vision in 3 projects, Meta Quest pro, HTC Vive Pro and HoloLens 2 once each). At least four of the participants only provide the XR software while their clients use their own HMDs. As a result, P7, P8 and P9 leave the choice of the specific hardware to the client, while others like P4 imposed a specific model (or several) to their clients. In both cases, the most commonly used headsets were the Meta

Quest 2 and 3. The main reasons identified by the participants for the prevalence of Meta headsets in the projects are their lower price compared to the rest of the HMD market (P7), or the interface usability (P11).

General barriers. P7, P8, P9 and P12 also mentioned a general skepticism towards VR, and subsequent difficulties in getting involvement from potential partners or the stakeholders in their field. In this respect, P8 refers to “*a lack of ‘exposure therapy’ for decision makers*”, leading to them “*not really seeing the point*”, yet. P12 refers to it as “*a chicken and egg problem*” when they explain that “*we haven’t achieved the stage where this is going to be used over time, self-initiated (. . .) We go through simulations and iteratively develop with users (. . .) get insights into potential avenues, where VR can deliver value.*”. However, the reluctance encountered when introducing the general public to XR was said to quickly fade once they actually tried the technology. As P7 pointed out, “*it’s really difficult to explain VR technology over Teams*”, but for P12, “*there may be some skepticism in general, but I find that once people actually take the VR headset on, the skepticism disappears quite a lot*”. Therefore, a broader adoption of XR outside of critical sectors was seen as a possible way to overcome this challenge. Another identified difficulty has to do with finding use cases where VR can add value (P9, P11, P12). This requires meaningful collaboration between actors with domain knowledge and XR developers. However, processes to support it are still partly lacking (P12). Additionally, P9 discussed the lack of funding for VR development in Norway: “*Currently, I don’t think there’s enough money going into it in Norway — so I don’t see Norway being in the forefront of this*”.

4.4 Security and privacy concerns in the XR ecosystem

Overall, we found that the security and privacy concerns of the participants did not necessarily reflect the ones expressed in the literature. No mentions were made of attacks exploiting VR-specific mechanisms (e.g., perceptual manipulations on redirected haptics), and the safety risks related with the user’s environment were not perceived as an issue by the interviewees.

Intrusions. P8, whose company provides a cloud-based service, noted that they often experienced intrusion attempts: “*I’d say there’s always someone trying to get in. There’s always something happening, but nothing major, luckily*”.

Asset protection. P13 raised concerns about the hardware and physical security offered by VR headsets: “*Authentication is just part of the question, but the memory chip is right there. So you could well just extract the memory chip, plug it into a reader and then extract the files including the 3D assets*”. P10 also mentioned assets being extracted as a potential issue and P12’s organization did not allow certain digital assets to be stored on the headset for this reason.

Intrusive data collection. While Meta HMDs were used in a least 9 of the organizations, 5 participants explicitly raised concerns about the privacy associated with the use of those headsets. In particular, P7, P9, P10 and P11 mentioned that the lack of insights into which data are captured and where it is stored was problematic. P7, P9 and P11 also expressed concerns about the extent to which the stated privacy policies are actually respected.

4.5 Current practices and barriers for security and privacy

While security was mentioned as a relevant concern several times, we found that there were few proactive efforts to guarantee the security and privacy of the products. Several reasons were provided to explain this.

Lack of maturity. P10 related this to the relative immaturity of the XR ecosystem. On security solutions for XR, P13 observed: *“We’re still in the early days. I don’t think there’s like very robust and time proven solutions out there.”*. P10 also noted that the current level of security can also be explained by the lack of critical assets to protect on the device: *“It’s not like military grade security — so it’s not any secrets that an enemy state can find, for example, by getting hands on that program”*. However, P7 mentioned that privacy risks were preventing the organization from implementing certain functionalities (e.g., hand or eye tracking) which could improve the solution’s efficiency or User Experience: *“There are several features that would improve the user experience, but at the cost of privacy (...) too much effort or risk on the privacy versus the benefit of implementing it”*.

Norms and regulations. None of the developed XR solutions reported in the questionnaire have been certified for a specific norm. Most interviewees also reported that there are currently no XR-specific norms or regulations relating to security or privacy that they have to comply with. However, both in the questionnaire and in the interviews, it was indicated that compliance with GDPR is required for those who collect personal data. Depending on the sector of use and the characteristics of the XR solution developed, there were also specific norms and requirements. For instance, P7’s company had to perform a security risk analysis, to be able to sell their healthcare-oriented training to municipalities. Other interviewees mentioned the Norwegian National Security Authority (NSM) security principles. P12, working in one of the larger organizations, also had to perform a security risk assessment of the used HMDs to guarantee compliance with the company’s internal security rules. Further, P8 mentioned a project with the ministry of foreign affairs in the context of the Russia-Ukraine war, which required full encryption of the entire solution. Some of the participants expect mandatory norms to change in the coming years: *“I think ISO certification is definitely on the table for us because it will be a requirement — it’s just a question of when”* (P8). The same interviewee also mentioned that their solutions will most likely need to comply to the USA-originating Cybersecurity Maturity Model Certification (CMMC) in the near future. P11 also noted that more norms or regulations on the HMD market (e.g., Meta, ByteDance) could be fundamental to protect the privacy of users.

Limited resources. When asked in the questionnaire whether privacy and security were taken into account, only one 1 of 6 respondents indicated that they were not particularly focused on it. Other respondents provided examples of how they focus on privacy and security, such as user anonymization, data onboarding, or using regular measures to ensure data privacy, authentication and data security measures as for any other software. P12 gave an example of safe login procedures, as a result of stricter compliance rules enforced by

the company, resulting in certain non-compliant HMDs being currently out of use. In the interviews, P10 also mentioned the HMDs being isolated from the organization’s network.

In the projects at earlier phases (often in research institutions), the security and privacy concerns were mostly ignored — the focus of such projects was rather to validate the functionality or relevance of XR in a specific context. Conversely, the more mature projects in most organizations have identified a person responsible for the security of the products, often the CTO (e.g., P6, P7 and P8), but their role is usually not limited to security and they have other responsibilities. To deal with the complexity of security and privacy, only P7 referenced the involvement of a security specialist in the XR project: *“We did it very thoroughly, with the security advisor that we have had as a consultant (. . .) they were helping us cover everything — there were so many different parts”*.

5 Discussion and conclusion

We conducted this study to explore different use cases for XR in critical sectors in Norway, and to understand how security and privacy are currently accounted for. These findings are non-exhaustive. While follow-up work is needed to validate them, overall, they show that XR holds a significant potential for Norway’s critical sectors, although the current ecosystem is still young. Interestingly — despite the limited sample size — we could observe a large breadth in the sectors represented. However, while XR is applied for various purposes, most of the reported projects revolved around learning or training (e.g., of employees). Moreover, while the examples show that XR is used in critical sectors at different scales, we captured no examples where XR is used for actual critical operations.

In terms of characteristics of XR use, we further found that Meta headsets were used in at least 9 of the organizations, while there were reservations in trusting Meta to respect the privacy of their users. All participants justified this paradox by pointing to the lower cost, especially considering the functionality of the product. At the same time, P9 mentioned that their criticized data collection practices seem to be the very reason that Meta is able to make the technology available at a low cost, which is necessary for a broader acceptance of XR.

Our findings also show that while security and privacy are considered as important, they are not a driving concern yet, as aspects such as affordability, resistance, and the lack of “killer applications” currently seem to be more pressing barriers to the larger-scale adoption of XR. Some of the participants ascribed this to the novelty of using XR in the Norwegian industry. The integration of XR in critical sectors is still relatively immature and organizations are still assessing the ecosystem and possibilities the technology can offer.

The lack of robust security solutions mentioned by the participants calls for more research focus on usable security solutions for critical sectors, for example authentication. At its current level, XR may not demand a larger focus on security and privacy, as the amount of sensitive data is limited, if not nonexistent, in most of the current use cases. However, in some solutions, the use of eye-tracking,

artificial intelligence or more detailed haptic devices appeared as prospective enhancements to the experiences. Privacy and security concerns associated with a broader range of XR functionalities will therefore need to be addressed more profoundly before the technology can be leveraged in operations. Future research could provide guidelines towards security and privacy in XR. Further, trade-offs between security, privacy and functionality were identified, both regarding the type of devices used and the amount of data collected. In the future, a better understanding of such trade-offs would be necessary to find ways to resolve them without having to compromise on improvements in the UX.

Acknowledgments. We would like to thank all participants and acknowledge all colleagues who helped with recruitment and pre-testing the questionnaire, in particular Shubham Jain. This work has received funding from the PERSEUS project, a European Union’s Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 101034240, and from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NOR-CICS) project no. 310105.

References

1. Adriana Cárdenas-Robledo, L., Hernández-Uribe, Ó., Reta, C., Antonio Cantoral-Ceballos, J.: Extended reality applications in industry 4.0. – a systematic literature review. *Telematics and Informatics* **73** (2022)
2. Aljerais, A., Barati, M., Rana, O., Perera, C.: Privacy laws and privacy by design schemes for the internet of things: A developer’s perspective. *ACM Comput. Surv.* **54**(5) (may 2021)
3. Cradit, N., Aguinaga, J., Hayward, C.: Surveying the (virtual) landscape: A scoping review of XR in postsecondary learning environments. *Education and Information Technologies* **29**, 8057–8077 (2024)
4. Cramer, H.S.M., Evers, V., Zudilova, E.V., Sloot, P.M.A.: Context analysis to support development of virtual reality applications. *Virtual Reality* **7**, 177–186 (2004)
5. Ergonomics, T.C.I.: ISO 9241-11:2018: Ergonomics of human-system interaction (11 2018)
6. Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., Akil, M.: Stakeholder perspectives and requirements on cybersecurity in europe. *Journal of Information Security and Applications* **61**, 102916 (9 2021)
7. Guzman, J.A.d., Seneviratne, A., Thilakarathna, K.: Unravelling spatial privacy risks of mobile mixed reality data. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **5**(1) (Mar 2021)
8. Hupont Torres, I., Charisi, V., De Prato, G., Pogorzelska, K., Schade, S., Kotsev, A., Sobolewski, M., Duch Brown, N., Calza, E., Dunker, C., Di Girolamo, F., Bellia, M., Hledik, J., Nai Fovino, I., Vespe, M.: Next generation virtual worlds: Societal, technological, economic and policy challenges for the eu (2023)
9. ISO: Iso 13407: Human-centred design processes for interactive systems (1999)
10. Karaosmanoglu, S., Cmentowski, S., Nacke, L., Steinicke, F.: Born to run, programmed to play: Mapping the extended reality exergames landscape. In: *Conference on Human Factors in Computing Systems - Proceedings* (2024)

11. Kupin, A., Moeller, B., Jiang, Y., Banerjee, N.K., Banerjee, S.: Task-driven biometric authentication of users in virtual reality (vr) environments. In: Kompatsiaris, I., Huet, B., Mezaris, V., Gurrin, C., Cheng, W.H., Vrochidis, S. (eds.) *MultiMedia Modeling*. pp. 55–67. Springer International Publishing, Cham (2019)
12. Maguire, M.: Context of use within usability activities. *International Journal of Human-Computer Studies* **55**, 453–483 (10 2001)
13. Miller, M., Herrera, F., Jun, H., Landay, J., Bailenson, J.: Personal identifiability of user tracking data during observation of 360-degree vr video. *Scientific Reports* **10** (10 2020)
14. Moore, A.G., McMahan, R.P., Dong, H., Ruoizzi, N.: Personal identifiability of user tracking data during vr training. In: *Proceedings - 2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, VRW 2021*. pp. 556–557. Institute of Electrical and Electronics Engineers Inc. (3 2021)
15. Mota, F., Braga, L., de Souza, C., Lopes, R.: Mapping the global technological landscape of virtual reality in education: a bibliometric and network analysis. *Social Network Analysis and Mining* **14** (2024)
16. Nair, V.C., Munilla-Garrido, G., Song, D.: Going incognito in the metaverse: Achieving theoretically optimal privacy-usability tradeoffs in vr. In: *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology. UIST '23*, Association for Computing Machinery, New York, NY, USA (2023)
17. Nettskjema: <https://nettskjema.no>, accessed September 24 2024
18. Odeleye, B., Loukas, G., Heartfield, R., Sakellari, G., Panaousis, E., Spyridonis, F.: Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers and Security* **124** (1 2023)
19. Rudschies, C., Schneider, I.: Ethical, legal, and social implications (elsi) of virtual agents and virtual reality in healthcare (1 2024)
20. Stefan, H., Mortimer, M., Horan, B.: Evaluating the effectiveness of virtual reality for safety-relevant training: a systematic review. *Virtual Reality* **27**, 2839–2869 (2023)
21. Subramanian, S., De Moor, K., Fiedler, M., Koniuch, K., Janowski, L.: Towards enhancing ecological validity in user studies: a systematic review of guidelines and implications for qoe research. *Quality and User Experience* **8**, 6 (2023)
22. The Council of the European Union: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. *Official Journal of the European Union* (2022)
23. Tseng, W.J., Bonnal, E., McGill, M., Khamis, M., Lecolinet, E., Huron, S., Gugenheimer, J.: The dark side of perceptual manipulations in virtual reality. In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery (2022)
24. Valluripally, S., Frailey, B., Kruse, B., Palipatana, B., Oruche, R., Gulhane, A., Hoque, K.A., Calyam, P.: Detection of security and privacy attacks disrupting user immersive experience in virtual reality learning environments. *IEEE Transactions on Services Computing* **16**(4), 2559–2574 (2023)
25. van Wyk, E., de Villiers, R.: Usability context analysis for virtual reality training in south african mines. In: *Proceedings of the 2008 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries: Riding the Wave of Technology*. p. 276–285. SAICSIT '08, Association for Computing Machinery, New York, NY, USA (2008)
26. XR Norge: <https://xrnorge.no/om-xr-norge/>, accessed September 24 2024