University of Tartu
Institute of Computer Science
Cybersecurity Curriculum

Joosep Parts

Cyber security risks in telepresence robotics within higher education and their mitigation

Master's Thesis (21 ECTS)

Supervisor: Kaido Kikkas, PhD

Tartu 2023

Cyber security risks in telepresence robotics within higher education and their mitigation

Abstract:
Telepresence robotics (TRPs) have become increasingly popular, particularly in higher education systems, as they enable users to remotely partake in events. However, this increased usage also presents potential security risks specific to TRPs, such as cyber-physical risks, and exposure of sensitive data among other risks. Current state of art does not adequately address these unique concerns, leading to a gap in understanding and mitigating TRPs related cybersecurity risks. This thesis aims to map potential security issues, offer mitigation strategies for found weaknesses, and bridges the gap by conducting case studies and expert interviews. This research will provide organizations utilizing TRPs with a better understanding of security risks and effective solutions to protect their systems and users.

Keywords: Cyber security, risk assessment, telepresence robotics

CERCS: T120 System technology, computer technology

Küberturvalisuse riskid kaugosalus robootikas kõrgharidussüsteemis ja nende vähendamine

Lühikokkuvõte:
Kaugosalus robotid on muutunud üha populaarsemaks, eriti kõrgemas haridussüsteemis, kuna need võimaldavad kasutajatel osaleda üritustel kaugjuhtimise teel. Siiski kaasnevad selle suurenenud kasutamisega ka kaugosalus robotitele omased potentsiaalsed turvariskid, nagu näiteks küber-füüsiline kohalolek ning tundliku info lekke. Praegused riskihindamise mudelid ei käsitle piisavalt neid ainulaadseid probleeme, ning on olemas lünk seotud riskide mõistmisel ja nende leevendamisel. Käesoleva magistritöö eesmärk on kaardistada potentsiaalsed turvaprobleemid ja pakkuda leitud nõrkuste leevendamiseks strateegiaid ning ületada lünk, viies läbi juhtumiuuringuid ja ekspert intervjuusid. See uurimus annab kaugosalus roboteid kasutavatele organisatsioonidele parema arusaama turvariskidest ja tõhusatest lahendustest nende süsteemide ja kasutajate kaitsmiseks.

Keywords: Küberturvalisus, riskianalüüs, kaugosalus robootika

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

List of Abbreviations and Terms

CC Cloud Computing

CS Computer Science

HE Higher Education

HEI Higher Education Institutions

ICSs Industrial Control Systems

ICT Information and Communication Technology

IoT Internet of Things

OWASP Open Web Application Security Project

ROS Robotic Operating System

ROS Robotic Operating System

SEN Special Education Needs

TRPs Telepresence robotics

UI User interface

Contents

List of Abbreviations and Terms **3**

1 Introduction **6**
1.1 Problem Statement 6
1.2 Objectives and Roadmap 6
1.2.1 Research Objective 6
1.2.2 Research Questions 6
1.2.3 Roadmap and Structure 8
1.3 Preliminaries 8

2 Background / State of the Art **9**
2.1 Related Work 10
2.2 Telepresence Robotics 14
2.3 Cyber Security Risks in Robotics 14
2.4 Cyber-physical Risks in Robotics 14
2.5 Cyber Security Risks in TRPs 14

3 Data Analysis **15**
3.1 Identified Security Risks in TPRs 15
3.2 Existing risk assessment and management strategies 15
3.3 Proposed Mitigation Strategies 15

4 Case Study: TalTech IT College (ICO) **16**
4.1 Context and TRPs Deployment 16
4.2 Results and Findings 16
4.3 Recommendations 16

5 Expert Interviews **17**
5.1 Participant Selection 17
5.2 Interview Results 17
5.3 Expert Validation and Proposed Solutions 17

6 Contribution **18**
6.1 Research method 18
6.2 Search strategy 18
6.3 Selection of primary and secondary studies 21
6.4 Extracted data 23

7 Validation **24**

7.1 Experimental validation 24

8 Conclusion **25**
8.1 Summary 25
8.2 Implications for TRPs Users and Organizations 25
8.3 Limitations and Future Research 25

References **27**

Appendix **28**
I. Data collected from case study 28
II. Interview Guide and Consent Form 29
III. Licence 30

1 Introduction

1.1 Problem Statement

With the increasing popularity of TRPs in higher education systems, enabling users to remotely partake in events, new security risks which could be characterized specific to TRPs have emerged [1–4]. These risks include abuse of privilege, unauthorized access, cyber-physical risks, and exposure of sensitive data among other risks [3, p. 120]. However, current risk assessment models do not adequately address these unique concerns, resulting in a knowledge gap in understanding and mitigating TPR-related risks [3]. This master's thesis aims to explore potential security issues associated with TRPs and propose methods to mitigate them by reviewing the state of art, conducting case studies and interviewing experts.

The research will involve identifying and validating potential risks through case studies and expert interviews, with a focus on identifying cybersecurity risks TRPs may pose to higher education systems. By proposing mitigation strategies and emphasizing cybersecurity, this study seeks to provide organizations utilizing TRPs with a better understanding of security risks and effective solutions to protect their systems and users. Ultimately, this research will contribute to bridging the gap between existing knowledge and the unique security concerns presented by the growing use of TRPs in higher education systems.

1.2 Objectives and Roadmap

1.2.1 Research Objective

The primary objective of this thesis is to identify cybersecurity risks related to organizations using TRPs and propose mitigation strategies to reduce the identified risks, focusing on user data security.

1.2.2 Research Questions

RQ: To what kind of security risks are organisations using TRPs exposed to, and how to mitigate the risks?

The main research question is divided into three different how questions, the potential security risks posed by TRPs, how organisations have assessed the potential risks and the solutions that can be provided to reduce the identified risks. The following sub-research questions are formulated in sequential order according to their importance:

1. **RQ1**: What are the potential security risks posed by TRPs, and how do these risks uniquely impact organizations utilizing these systems?

2. **RQ2**: How have organizations implemented assessment and management strategies to address cybersecurity risks associated with telepresence robotics?

3. **RQ3**: What potential solutions can be provided to reduce identified security risks?

RQ1: Identification of potential security risks posed by TRPs is the first step. In this step the possible security risks will be identitified by analyzing existing frameworks, migigation strategies and previous works in the field. This sub-research question focuses on uncovering the distinct security risks associated with telepresence robotics and examines their implications for organizations that deploy TRPs. By identifying these risks, the research will contribute to a comprehensive understanding of the challenges and vulnerabilities that need to be addressed in order ensure secure operation of TRPs systems. This exploration will consider various aspects of TRPs, such as remote connectivity, cyber-physical presence, and live video and audio feeds, to highlight the unique security concerns that arise from their use. Additionally, the research will investigate how these risks may differ from those faced by organizations using other types of robotics and what factors contribute to the increased vulnerability of TRPs systems.

RQ2: Once we have identified possible security risks the next step is to examine how have organizations implemented assessment and management strategies to address cybersecurity risks associated with TRPs? This sub-research question focuses on understanding the mechanisms and processes involved in managing TRPs systems. Finding the issues and gaps in current implementation is important to validate found security risks from teoretical material, but is also important before appropriate mitigation strategies can be considered. Addressing this question is essential for identifying potential vulnerabilities and areas where security improvements can be made.

RQ3: Following the identification of security risks associated with TRPs, this sub-research question concentrates on investigating and proposing potential mitigation strategies that effectively address the recognized risks. The study will explore a range of solutions, including technological advancements, policy implementation, and organizational practices, to provide a comprehensive understanding of how organizations can secure their TRPs systems. The proposed solutions should be practical, effective to the needs of organizations using TRPs. This will involve considering the unique security risks posed by TRPs and the distinct contexts in which they are deployed. The focus will be on user data security and the interaction between external users and TRPs, ensuring that the proposed mitigation strategies safeguard sensitive information and maintain the privacy and security of all parties involved.

By addressing these three sub-research questions, the thesis aims to provide a comprehensive understanding of the security risks faced by organizations using TRPs and offer practical solutions for mitigating these risks, ultimately contributing to a more secure and reliable TRPs environment.

1.2.3 Roadmap and Structure

To achieve the research objective, the following roadmap and structure will be followed:

1. Literature Review and analysis: A comprehensive review of existing research on TRPs, risk assessment models, and related frameworks will be conducted to identify potential issues within TRPs systems.
2. Case Studies: Case studies will be conducted to validate existence of possible security risks by analyzing real-life scenarios involving TRPs usage in organizations;
3. Expert Interviews: Interviews with technical staff who have experience in integrating TRPs into organizations will be conducted to confirm the identified risks and explore possible mitigation strategies proposed by the experts;
4. Data Analysis and Proposed Mitigation Strategies: The findings from case studies and expert interviews will be analyzed to identify potential security concerns and risks posed by TRPs, as well as potential solutions to these risks;
5. Conclusion: The thesis will conclude by summarizing the key findings, discussing the limitations of the research, and suggesting avenues for future research.

Following this roadmap, the thesis will contribute to bridging the gap between existing cybersecurity knowledge regarding robotics in higher education systems and the unique security concerns presented by the growing use of TRPs.

1.3 Preliminaries

2 Background / State of the Art

The rapid growth of technology, multimedia, and robotics has led to significant advancements in Information and Communication Technology (ICT) infrastructure worldwide, prompting the development of various educational programs. The evolution of technology has boosted the field of robotics, resulting in a wide array of potential applications in Higher Education (HE). In recent events, COVID-19 has expedited the adoptation of robotic techonology, including TRPs into our lives [5, p. 193]. The use of robotics in education is increasing, with TRPs being applied in Higher Education Institutions (HEI) and other diverse roles in the industry [6; 7].

TRPs have great potential for pedagogic reasons within education at all levels, as they benefit HE personnel the replacement of physical presence and allow students with Special Education Needs (SEN) to have access to HE they might miss otherwise due to their disabilities [6, p. 546]. They can also provide a more engaging experience when normal cicumstances for interaction are not possible (COVID-19 restrictions) [5, p. 197] [7, p. 1]. TRPs have ability to create interaction between individuals which can be an opportunity for learning not only from a three-dimensional inanimate object but also through interaction with other people. This interaction enables TRPs to aid in improving social skills in individuals with disabilities [6, p. 541].

Although the advantages of TRPs in education are numerous, this technology also creates new possible security risks that need to be assessed. Interconnectivity with TRPs by the internet to the HEI means that the organization needs to be aware of possible security risks [3, p. 120]. Cyber-physical threats could extend the range of known attack vectors by utilizing robotic capabilities and creating new attack surfaces not considered before [8, pp. 18–19]. Cybersecurity is crucial in HEI due to the vast amount of computing power and access to other resources universities have. These institutions hold large volumes of personal, financial, and intellectual data that can be attractive targets for cybercriminals.

It is inherently difficult to ensure security within robotics systems due to the complexity of robotic systems in general, leading to wide attack surfaces and a variety of potential attack vectors [4, p. 2]. In addition, robotics manufacturers often struggle to mitigate vulnerabilities in reasonable time periods. The lack of investment in cybersecurity and the immature state of the field in robotics cybersecurity contribute to the challenges in securing robotic systems. Most current robots are vulnerable, and defensive approaches are struggling to keep up with the need for security [4, p. 12]. Therefore it is reasonable to assume that TRPs are also vulnerable to similar security risks. Though there exists various risk assessment models, frameworks, and methodologies to assess cybersecurity risks within robotics systems in general, the studies which focus on TRPs usage in HEI are limited and scattered.

Because of the lack of research on TRPs in HEI regarding cybersecurity risks and the usage of TRPs is increasing, this thesis aims to bridge the gap in the literature by providing a review of the state of the art of TRPs cybersecurity risks in HEI. We explore cyber-physical threats which could be apply to TRPs, and offer possible mitigation strategies for identified cybersecurity risks.

2.1 Related Work

The growing prevalence of robots in various domains, including homes, industries, and professional facilities, has led some to consider robotics the next technological revolution. The first recorded human death caused by a cyber-physical system dates back to 1979 [4, p. 2]. Even though much time has passed since then, evidence suggests that robotics security is being underestimated [9, pp. 1–2].

Over the past decade, security and cybersecurity have significantly expanded, drawing individuals to various sub-areas within security assessment. Recent technical reports indicate that most security researchers assess vulnerabilities in websites, mobile phones, and Internet of Things (IoT) devices [4; 10]. However, despite their relevance, robot vulnerabilities have not been formally studied or actively researched [4, p. 1]. This gap is attributed to the complexity of robot security from a technological standpoint, requiring an interdisciplinary mix of profiles [11, pp. 74–77], and the lack of guidelines, tools, and formal documentation for assessing robot security [2, p. 7].

Some works in the field attempt to analyze cybersecurity concerns within robotic systems in more technical terms. Categorizing security concerns into four categories: physical, network, OS, and application security [9, p. 5]. Yaacoub et al. analyzed the different layers more in-depth to expose possible security issues within the robotics system [3]. Fern ández and Matellán [12, p. 76] propose a model that integrates Open Web Application Security Project (OWASP) risk identification and various cyber-physical security aspects, considering the sources, targets, and potential consequences of robotic functionality. Mayoral-Vilches found that manufacturers lack the interest to invest in robotic systems security or that the systems' complexity exposes possible weaknesses [4]. The overall goal of these works is to provide insight for assessing security risks in robotics, and they overlap in most areas with somewhat consensus. However, there seems to be a lack of a common methodology for categorizing security risks in robotics. Though we do not have a clear consensus on how to characterize security risks, the methodologies presented can utilized to examine TRPs security concerns as they operate in the same domain of service robotics.

To generalize, there exists three domains of risk in robotics: physical, cyber and cyber-physical. Physical risks include threats that affect the robot's operation mode, such as destruction, partial damage, disruption, degradation, or unexpected behavior. These

threats can arise from natural disasters, accidents, or attacks. Cyber risks are threats that impact the robot's information, such as data gathered, stored, or transmitted. They can be related to issues in the robot's software, third-party libraries, or general vulnerabilities in the software components. Software flaws, security configuration issues, or software feature misuse can cause these risks. Cyber-physical risks combine both physical and cyber threats. These threats can compromise sensors or actuators by substituting or modifying hardware or firmware, adding new hidden functionality. The impact of these threats is unexpected as the original functional definition is compromised [12, pp. 77–78]. These risks can affect various actors involved in deploying robotic systems, such as final users, business users, robot vendors, and independent software developers.

Physical threats, even in smaller robotic systems, should still be considered a possibility. TRPs are not immune to the risks mentioned above. Like any electronic device, there is a possibility for malfunction, which can lead to the device being inoperable or even becoming dangerous (fire, explosion). In the event of an accident that results in damages It will raise legal questions regarding who is liable for the damages to property or injury to a person. It has been argumented that though the producer of the robot is responsible for the safety of the robot, and the operator is responsible for the safety of the environment in which robot operates [13]. Little Red Riding Hood, while journeying through the forest to visit her grandmother, encountered a sly wolf, leading to a dangerous yet ultimately triumphant adventure. In a less extreme scenario, the robot's unexpected inoperability can cause a loss of confidence in the system or deprive the user of the benefits of the system as users vary of failures of robots [7, pp. 9–10]. Physical threats by the robotic systems to human users are not limited to just direct contact. Robotic system could alter the environment, which can affect the user's safety.

The levels of physical attacks are categorized as destruction, partial damage, degradation, disruption, or substitution. These threats are further differentiated according to the type of user, namely domestic/personal, commercial/business, and public administration [12, p. 80]. Despite the significance of physical threats, privacy risks often emerge as the most relevant concern for service robot users. Though the physical damage caused by service robots may be limited due to their size, information leaks can lead to severe consequences [12, p. 83]. Physical threats can also be linked to psychological harm [14, p. 5].

Robotic system psychological risks refer to the potential adverse effects on users' mental well-being that may arise from interacting with robotic systems. These risks can occur when a robot's behavior is modified or malfunctions, and users may not notice these changes or misinterpret them as normal behavior. Furthermore, cybersecurity attacks on robotic systems can also impact their task performance and endanger users' safety without being apparent to the user, further contributing to psychological risks [14, p. 5]. This area might become even more relevant in the future as some researchers

are investigating possibilities to create more meaningful interactions and emotional connections between humans and robots [21, p. 186].

Cyber threats to HEI according to Verizon 2022 Data Breach Investigation Report (DBIR), are external (75%) threat actors who leverage system intrusion and web application attacks (80%) to penetrate a system and target personal data (63%) or credentials (41%) [10, p. 57]. Latest reports, however, have not indicated specifically that cyber threats through TRPs are a threat to HEI in particular. Though, we do not have such recorded cases analyzed in academic literature, the theoretical possibility of such an attack is not far-fetched, as we know that robotic systems have limitations. Cyber threats imply that the robotic system can be the source of threats, and the robot's software is vulnerable to attacks. Robotic systems face numerous threats that target their security, classified into various categories such as wireless jamming, reconnaissance and scanning, information disclosure, abuse of privilege, information gathering, information interception, information modification, physical damage, service disruption or denial, sabotage and espionage, and tracking and monitoring [3, p. 122]. These threats also compromise the CIA triad—Confidentiality, Integrity, and Availability—of traditional and advanced Industrial Control Systems (ICSs), as well as the Cloud Computing (CC) domain associated with the robotic field [3, p. 116]. It is crucial to address these threats to ensure the protection, privacy, and proper functioning of robotic systems.

When discussing cyber threats, we must consider whether privacy is part of that security. A classification of privacy risks associated with robotic sensors is proposed, revealing that sensor data fusion poses the highest privacy risk due to the potential disclosure of personal activities. Exteroceptive sensors, particularly cameras, and microphones, are also significant privacy concerns, while the range and proprioceptive sensors are less critical. Furthermore, processing sensor data "in the cloud" introduces additional risks in communication and data storage, necessitating careful consideration of legal and ethical implications [12, pp. 82–84].

Privacy is a fundamental human right and a key component of HEI. Modern TRPs Double 2 provides privacy features such as end-to -end 128-bit AES Encryption [6, p. 544]. However, users of TRPs and students around such devices are still concerned for their privacy noting that privacy and control methods are the most important when building trust towards TRPs [15, p. 59]. This is a reasonable concern because technological data security does not guarantee privacy. How can the user identify if the robotic system is recording or transmitting data without consent? Technological failures in the user's inability to identify when it is being recorded is not a new phenomenon [16].

Robotic systems can be attacked through the network, the robot's software, or the robot's hardware. They are prone to vulnerabilities in robotic systems' communications and the potential attacks could impact security services such as authentication, confidentiality,

and integrity. These attacks range from jamming and de-authentication attacks, which disrupt communication and control, to traffic analysis and eavesdropping attacks that compromise privacy and confidentiality. Other attacks, such as false data injection, denial of service, and man-in-the-middle attacks, target the availability, integrity, and authentication of robotic systems [3, pp. 126–128]. It is crucial to protect robots from potential attacks by employing robust authentication processes, lightweight cryptographic algorithms, privacy-preserving techniques, and non-cryptographic solutions [3, pp. 147–149]. To protect the robot from being compromised it is suggested to apply privacy by design principles in the development phase of the robotic system [3; 17; 21].

But not only are robotic systems vulnerable, users can become vulnerable though the robotic system. For example, Robot Operating System (ROS) can be manipulated to overtake the system and control the robot in a physical way or to manipulate its sensors/data [17].

Cyber-physical threats are a combination of both physical and cyber threats. Critical differences between TPRs and other robotics are how users can interact with the robot, and through the robotic system, they can interact with the environment. Previously established cyber attack vectors within the robotics system could now be exploited in ways that have not been considered before, creating a new dimension of cyber -physical threats, which are not limited to just cyber or physical threats. This creates the need to analyze this new domain of possible attack vectors and ultimately enhance existing knowledge of cyber-physical security.

Extending the definition of cyber-physical threats, when the terminology is used in the context of robotic systems, it usually refers to the direct physical threat from the machine to the user. Such is the first human death caused by a robot in 1979 [9, p. 2]. That example could be considered as a direct (cyber)physical threat. “cyber“ refers to the fact that one of the parties involved in the accident was a robot and the “physical“ part to the fact that direct physical contact between the robot and the human was made. In the context of cyber-physical threats regarding TRPs, we should also examine this domain in the realm of a robot having access to sensitive information through its systems(audio and video capabilities) but also physical access to the environment and the ability to manipulate it (movement, touch) [17, p. 982] [18, p. 250] [8, p. 11]. Though the context is different (robot → human vs. robot → environment → human), and sense of danger might not be as imminent, cyber-physical threats still exists in TRPs and needs to be addressed [19, p. 2].

In that sense, cyber-physical threats could be interpreted as a combination of three different sub-categories of risks:

1. Cyber-physical (P – physical) threats are direct physical threats from the robot to the user.

2. Cyber-physical (E – environment) threats in which the robot can access the environment and manipulate it.
3. Cyber-physical (C – cyber) threats in which the robot capabilities are used to extend the known cyber attack surface.

In order to introduce new terminology, we will use the following notation to refer to the three sub-categories of cyber-physical threats : P – physical, E – environment, C – cyber. To address these possible cyber-physical (PEC) risks within TRPs, we propose a systematic methodology to investigate the existence and importance of such risks. By conducting a case study, we will be able to verify the existence of such risks and interview experts to determine the importance of the risks and gain insight into the possible mitigation strategies. We argue that cyber-physical(PEC) risks in TRPs should be acknowledged as a significant concern in the field and raise awareness of such threats within the TRPs systems. By proposing new terminology with mitigation strategies and a systematic methodology to investigate the existence and importance of such risks, we hope to contribute to the field of TRPs security and privacy within the HEI and for organizations utilizing TRPs in general.

2.2 Telepresence Robotics

2.3 Cyber Security Risks in Robotics

2.4 Cyber-physical Risks in Robotics

2.5 Cyber Security Risks in TRPs

3 Data Analysis

3.1 Identified Security Risks in TPRs

3.2 Existing risk assessment and management strategies

3.3 Proposed Mitigation Strategies

4 Case Study: TalTech IT College (ICO)

4.1 Context and TRPs Deployment

4.2 Results and Findings

4.3 Recommendations

5 Expert Interviews

5.1 Participant Selection

5.2 Interview Results

5.3 Expert Validation and Proposed Solutions

6 Contribution

6.1 Research method

Primarily focus is on exploring and understanding the cybersecurity risks, and the underlying perspectives of the participants involved in HEI where TRPs have been deployed. Given the nature of the study, the absence of known empirical data, and the limited time for conducting case studies, a qualitative research approach will help to gain deeper insights. Thus it is important to develop a review protocol which sets the framework for conducting a thorough and unbiased review of the literature [20, p. 8]. It ensures that systematic and rigorous approach is followed, which enhances the credibility and reliability of the review. Following review protocol steps helps to minimize the risk of bias in the review process by establishing predefined criteria for study selection, quality assessment, and data extraction:

1. Establish the background and context of the study;
2. Formulate clear and specific research questions;
3. Define the search strategy, including search terms and resources to be used;
4. Set the study selection criteria and procedures;
5. Develop study quality assessment checklists and procedures;
6. Design a data extraction strategy tailored to the research questions;
7. Plan the synthesis of the extracted data, including descriptive and quantitative methods, as appropriate;
8. Outline a dissemination strategy for the review findings;
9. Set a project timetable to ensure timely completion of the review [20, pp. 4–5].

6.2 Search strategy

Search strategy was developed to identify relevant literature for this review following the search strategy generation guidelines [20, pp. 7–8]. Search strategy for the following thesis consists of 3 steps:

1. Generation of keywords and search terms;
2. The use of search filters;
3. Selection of credible sources.

Keywords: Initially, the search keywords were created by breaking down the research questions into their main concepts. A list of search terms and phrases related to each key concept was generated by applying term harvesting to each research question. Main keywords were complemented by secondary keywords (synonyms), alternative spellings, and related terms to ensure a comprehensive search. The result was a list of search terms and phrases used to query the databases. To narrow down the search, the terms were combined using Boolean operators (where applicable).

Table 1. Selected keywords and synonyms

Primary keywords	**Secondary keywords**
telepresence	telerobotics, tele-education
robotics	robot
cybersecurity	cyber, security, digital
risks	compromise, assessment, threats
education	organization

Filters: The search filters were used to limit the search to the relevant studies. Most common filters used were: publication date, type of publication, discipline and language. The filters were applied to the search results to ensure that only relevant studies were included in the review. Most important filter being the publication year. The search was limited to the last 10 years (2014-2023) to ensure that only the most recent and relevant studies were included in the review. Primary studies were limited to maximum age of 5 years and secondary studies to maximum age of 10 years. Search filters of primary studies complemented the secondary seach filters. Secondary studies were extended to other languages than English (incl. Estonian).

Table 2. Used search filters

Primary studies			**Secondary studies***		
Date Range	Type	Discipline	Date Range	Type	Discipline
2019...2023	Reports, Journals, Experiments, Datasets	Computer Science, Engineering	2014...2023	Articles, Conference Proceedings, Whitepapers	Social Sciences, Psychology

* Includes primary search terms

Sources: After conducting preliminary searches using chosen search terms, and filters in the selected resources, search queries were refined as needed to obtain required materials. Preliminary searches showed that using main keywords in serch strategy produced large number of results but highly relevant studies, thus the use of secondary keywords was not optimal in search for primary studies. Record the search terms used and the number of

results obtained from each resource was recorded for later use to check for updates on the subject. Most filtering refinements were done in User interface (UI). To identify relevant research several databases were queried with the same search terms. Database selection was based on the main category of hosted works (technology) as indicators show that most TRPs related materials originate from Computer Science (CS) field [15, p. 62], the number of publications published and the age of the portal. In the execution phase main databases were (SpringerLink, IEEExplore, Scopus, ScienceDirect, Web of Science) due to their large number of publications and relvance on the topic. Initial queries yeilded small number of results, thus the search was extended to secondary sources (LISTA, Frontiers, Google Scholar).

Table 3. Selected sources in order of relevance

	Publisher	**Year**	**Topics**
1	SpringerLink	1996	Computer Sciences, Engineering, Environment
2	IEEExplore	2000	Computer Sciences, Electrical Engineering and Electronics
3	Scopus	2004	Physical Sciences, Life sciences, Social Sciences
4	ScienceDirect	1997	Physical Sciences and Engineering, Life Sciences
5	Web of Science	1998	Physical Sciences, Technology, Life Sciences &Biomedicine
6 *	LISTA	2005	Classification, Electronic resources and ERM systems
7 *	Frontiers	2007	Education, Computer Science, Robotics and AI
8 *	Google Scholar	2004	Various topics
9 *	Research Gate	2008	Computer Sciences, Engineering, Social Sciences

* Secondary sources

Search scope default language selection was English. Examples of search search string composition used with combination of search terms, filters on the selected resources can be seen in Table 4. The search string used all possible combinations. Preliminary searches showed that using main keywords yielded best results.

Table 4. Composition of search strings

	Search string
1	telepresence AND cybersecurity OR risks AND assessment AND robots AND education
2	tele-robotics AND cybersecurity AND risks AND robots OR education AND assessment AND compromise OR mitigation
3	telepresence AND cybersecurity AND risks AND assessment AND robots AND education AND management AND mitigation AND security AND compromise OR threats

The databases used in this study contained scientific journals, conference proceedings, books, and trade journal articles. In April 2023, the database search was conducted,

yielding a total of 926 publications. Some references were found in multiple databases. To eliminate duplicates, a unified list featuring the titles of the chosen publications was created. The abstracts of these publications were reviewed to confirm their relevance to TRPs and cybersecurity. After implementing this exclusion criterion, 10 publications were chosen for more in-depth analysis as seen in Table 5.

Table 5. Number of selected studies found and selected for analysis

		Journal		**Conference Papers**		**Book Chapter**		**Whitepaper**	
Year	**Total**	**T**	**S**	**T**	**S**	**T**	**S**	**T**	**S**
2014	14	6		6		2			
2015	10	5		3		2			
2016	7	6	1			1			
2017	18	12	2	5		1			
2018	32	22	1	3		6		1	
2019	63	39	1	15		9			
2020	104	68	2	16		20			
2021	250	122	5	40	1	88			
2022	306	116	5	59		131			1
2023	123	54		16		52		1	
Total:	927	450	17	163	1	312		2	1

* T - total, S - selected

6.3 Selection of primary and secondary studies

To identify primary studies that provide direct evidence about the research question, specific selection criteria was defined during the protocol definition stage. Although criteria was refined during the search process, it served as a foundation for identifying relevant studies. The selection criteria included factors such as study design, levels of evidence, and outcome measures, ensuring that the chosen studies directly addressed our research question [20, pp. 10–16]. TRPs in the context of cybersecurity and education is a relatively new field of robotics with most research starting from 2015. Therefore, the selection of primary studies was extended to include secondary studies that provide indirect evidence about the research question.

In the context of assessing cybersecurity risks in telepresence robotics for higher education systems, the literature analysis process identified 7 key findings that directly influence the assessment of cybersecurity risks in HEI or in other ways support the answering of research questions. Among these studies, it was taken into account that secondary studies within the timerange of 2014...2023 may have outdated information and as such their findings were noted and used as supportive information. Throughout

the discussion of each study, the aspects related to cyber security risks in TRPs are highlighted. Table 6 lists findings and the corresponding references:

1. Identification of security risks associated with TRPs.
2. Analysis of existing risk assessment models and their limitations in addressing TRPs-specific security challenges.
3. Potential security vulnerabilities in robotics, including hardware, software, and network-related issues.
4. Usage of TRPs in HEI.
5. Examination of studies that highlight TRPs security incidents and the effectiveness of implemented countermeasures.
6. Exploration of future research directions to enhance the security of TRPs in higher education and other settings.
7. Investigation of mitigation strategies and best practices to address identified weaknesses in TRPs security.

Table 6. Selected sources

#	Year	References	1	2	3	4	5	6	7
1	2021	Zhu et al. [11]	X	X			X		X
2	2021	Fosch-Villaronga et al. [19]	X	X					X
3	2022	Verizon [10]						X	X
4	2021	Lacava et al. [2]	X					X	
5	2022	Yaacoub et al. [3]	X	X	X		X	X	X
6	2020	Pessoa et al. [21]					X	X	
7	2021	Villaronga et al. [14]	X	X					X
8 *	2017	Lera et al. [12]	X	X	X			X	
9 *	2016	Sabine et al. [13]			X				
10 *	2018	Ahmad et al. [8]	X	X	X	X			X
11 *	2017	Portugal et al. [17]	X		X				
12 *	2022	Lei et al. [1]	X			X			
13 *	2022	Leoste et al. [7]				X			
14 *	2018	Vilches et al. [9]	X	X					
15 *	2022	Mayoral-Vilches [4]			X		X		
16 *	2020	Singar et al. [18]				X			X
17 *	2019	Reis et al. [6]				X			
18 *	2022	Virkus et al. [15]				X			
19 *	2021	Gupta et al. [5]				X			

* Secondary studies

6.4 Extracted data

7 Validation

7.1 Experimental validation

8 Conclusion

8.1 Summary

8.2 Implications for TRPs Users and Organizations

8.3 Limitations and Future Research

Time, resources, nr of case studies and access to experts are the main limitations of this research.

References

[1] M. Lei, I. Clemente, H. Liu, and J. Bell, "The acceptance of telepresence robots in higher education," *International Journal of Social Robotics*, vol. 14, pp. 1–18, Jun. 2022. DOI: 10.1007/s12369-021-00837-y.

[2] G. Lacava *et al.*, "Cybsersecurity issues in robotics.," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 12, no. 3, pp. 1–28, 2021.

[3] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, pp. 1–44, 2022.

[4] V. Mayoral-Vilches, "Robot cybersecurity, a review," *International Journal of Cyber Forensics and Advanced Threat Investigations*, 2022.

[5] A. Gupta, A. Singh, D. Bharadwaj, and A. K. Mondal, "Humans and robots: A mutually inclusive relationship in a contagious world," *International Journal of Automation and Computing*, vol. 18, pp. 185–203, 2021.

[6] A. Reis, M. Martins, P. Martins, J. Sousa, and J. Barroso, "Telepresence robots in the classroom: The state-of-the-art and a proposal for a telepresence service for higher education," in May 2019, pp. 539–550, ISBN: 978-3-030-20953-7. DOI: 10.1007/978-3-030-20954-4_41.

[7] J. Leoste, S. Virkus, A. Talisainen, K. Tammemäe, K. Kangur, and I. Petriashvili, "Higher education personnel's perceptions about telepresence robots," *Frontiers in Robotics and AI*, vol. 9, 2022, ISSN: 2296-9144. DOI: 10.3389/frobt.2022.976836. [Online]. Available: https://www.frontiersin.org/articles/10.3389/frobt.2022.976836.

[8] K. M. A. Yousef, A. AlMajali, S. Abu Ghalyon, W. Dweik, and B. J. Mohd, "Analyzing cyber-physical threats on robotic platforms," *SENSORS*, vol. 18, no. 5, May 2018. DOI: 10.3390/s18051643.

[9] V. M. Vilches *et al.*, "Introducing the robot security framework (rsf), a standardized methodology to perform security assessments in robotics," *CoRR*, vol. abs/1806.04042, 2018. arXiv: 1806.04042. [Online]. Available: http://arxiv.org/abs/1806.04042.

[10] V. D. B. I. Report, "2022 data breach investigations report," en, Tech. Rep., 2022, KerkoCite.ItemAlsoKnownAs: 2339240:XT3T7FLZ 2405685:SNEYNCSI. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/ (visited on 2022-06-15).

[11] Q. Zhu, S. Rass, B. Dieber, V. M. Vilches, *et al.*, "Cybersecurity in robotics: Challenges, quantitative modeling, and practice," *Foundations and Trends® in Robotics*, vol. 9, no. 1, pp. 1–129, 2021.

[12] F. Rodríguez Lera, C. Fernández, Á. Guerrero, and V. Matellán, "Cybersecurity of robotics and autonomous systems: Privacy and safety," in Dec. 2017, ISBN: 978-953-51-3635-4. DOI: 10.5772/intechopen.69796.

[13] S. Gless, E. Silverman, and T. Weigend, "If robots cause harm, who is to blame? self-driving cars and criminal liability," *New Criminal Law Review*, vol. 19, no. 3, pp. 412–436, Aug. 2016, ISSN: 1933-4192. DOI: 10.1525/nclr.2016.19.3.412. eprint: https://online.ucpress.edu/nclr/article-pdf/19/3/412/206818/nclr_2016_19_3_412.pdf. [Online]. Available: https://doi.org/10.1525/nclr.2016.19.3.412.

[14] E. Fosch Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law Security Review*, vol. 41, p. 105 528, Jul. 2021. DOI: 10.1016/j.clsr.2021.105528.

[15] S. Virkus, J. Leoste, K. Marmor, T. Kasuk, and A. Talisainen, "Telepresence robots from the perspective of psychology and educational sciences," *Information and Learning Sciences*, no. ahead-of-print, 2023.

[16] P. Kröger Jacob Leonand Raschke, "Is my phone listening in? on the feasibility and detectability of mobile eavesdropping," in *Data and Applications Security and Privacy XXXIII*, S. N. Foley, Ed., Cham: Springer International Publishing, 2019, pp. 102–120, ISBN: 978-3-030-22479-0.

[17] D. Portugal, S. Pereira, and M. S. Couceiro, "The role of security in human-robot shared environments: A case study in ros-based surveillance robots," in *2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN)*, 2017, pp. 981–986. DOI: 10.1109/ROMAN.2017.8172422.

[18] A. Singar and K. Akhilesh, "Role of cyber-security in higher education," in Jan. 2020, pp. 249–264, ISBN: 978-981-13-7138-7. DOI: 10.1007/978-981-13-7139-4_19.

[19] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Computer Law Security Review*, vol. 41, p. 105 528, 2021, ISSN: 0267-3649. DOI: https://doi.org/10.1016/j.clsr.2021.105528. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364921000017.

[20] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, Aug. 2004.

[21] M. Pessoa and J. Jauregui-Becker, "Smart design engineering: A literature review of the impact of the 4th industrial revolution on product design and development," *Research in Engineering Design*, vol. 31, pp. 1–21, Apr. 2020. DOI: 10.1007/s00163-020-00330-z.

Appendix

I. Data collected from case study

II. Interview Guide and Consent Form

III. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Joosep Parts**,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Cyber security risks in telepresence robotics within higher education and their mitigation,
   *(*title of thesis)

   supervised by Kaido Kikkas.
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Joosep Parts
10/04/2023