computers

MDPI

Review

A Systematic Review on Social Robots in Public Spaces: Threat Landscape and Attack Surface

Samson O. Oruma [1], Mary Sánchez-Gordón [1], Ricardo Colomo-Palacios [1,2,*], Vasileios Gkioulos [3] and Joakim K. Hansen [4]

[1] Faculty of Computer Sciences, Østfold University College, 1757 Halden, Norway
[2] Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid, 28660 Boadilla del Monte, Spain
[3] Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, 2802 Gjøvik, Norway
[4] RSS Department, Institute for Energy Technology, 1777 Halden, Norway
* Correspondence: ricardo.colomo-palacios@hiof.no or ricardo.colomo@upm.es

Abstract: There is a growing interest in using social robots in public spaces for indoor and outdoor applications. The threat landscape is an important research area being investigated and debated by various stakeholders. Objectives: This study aims to identify and synthesize empirical research on the complete threat landscape of social robots in public spaces. Specifically, this paper identifies the potential threat actors, their motives for attacks, vulnerabilities, attack vectors, potential impacts of attacks, possible attack scenarios, and mitigations to these threats. Methods: This systematic literature review follows the guidelines by Kitchenham and Charters. The search was conducted in five digital databases, and 1469 studies were retrieved. This study analyzed 21 studies that satisfied the selection criteria. Results: Main findings reveal four threat categories: cybersecurity, social, physical, and public space. Conclusion: This study completely grasped the complexity of the transdisciplinary problem of social robot security and privacy while accommodating the diversity of stakeholders' perspectives. Findings give researchers and other stakeholders a comprehensive view by highlighting current developments and new research directions in this field. This study also proposed a taxonomy for threat actors and the threat landscape of social robots in public spaces.

Keywords: social robots; humanoids; threat landscape; attack surface; public space; cybersecurity; privacy; safety

Citation: Oruma, S.O.; Sánchez-Gordón, M.; Colomo-Palacios, R.; Gkioulos, V.; Hansen, J.K. A Systematic Review on Social Robots in Public Spaces: Threat Landscape and Attack Surface. *Computers* **2022**, *11*, 181. https://doi.org/10.3390/computers11120181

Academic Editors: Osvaldo Gervasi and Bernady O. Apduhan

Received: 8 November 2022
Accepted: 6 December 2022
Published: 8 December 2022

1. Introduction

Social robotics is a rapidly growing technology with the potential to address some of our modern societal challenges [1]. The importance of social robots in today's society is evident from their ability to provide personalized human-like services in elderly care [2,3], general healthcare [4], hospitalized children care [5], mental healthcare [6], dementia care [7–9], education [10–13], language studies [14–17], entertainment [18], retail services [19], tourism [20], hospitality [21,22], public spaces [23–25], and during pandemics like COVID-19 [26,27] or in other possible cases. The social robotics market was valued at USD 1.98 billion in 2020 and will reach USD 11.24 billion in 2026 [28], with healthcare being the main driver. The European Union, in collaboration with industrial partners, is investing EUR 2.6 billion in ten years of research (2021–2030) for Artificial Intelligence (AI), data, and robotics [29], of which social robots represent a practical embodiment of all these technologies.

According to the United Nations (ESCAP), the number of older persons (60+) in 2021 is 651 m (14% of the global population), and it is estimated to rise to one quarter by 2050 [30]. This development attests to advances in medical healthcare; however, there is a serious concern, as the number of ageing people already outnumbers the number of children

younger than five years as of 2020 [31]. The shortage of competent and committed paid long-term elder care workers is an open challenge [32] that social robots can conveniently resolve. However, introducing social robots to public spaces has attracted several concerns from the research community, industry, policymakers, and other stakeholders, ranging from security, safety, privacy, ethical, legal, and technological concerns [25,33–37]. The security and safety of humans and the protection of the data collected by these social robots in public spaces are the foremost of all these concerns [38,39].

Social robots interact with humans and the environment through their numerous sensors and actuators, which are vulnerable to diverse attacks [40,41]. Most social robot processing functions are performed at the edge/cloud [42,43] through wireless communication links [44] due to limitations on battery capacity, physical space, and the systems' demanding storage and computational needs, which creates new attack surfaces for threat actors. When social robots are connected to the Internet, they are exposed to the same threats and vulnerabilities as other Internet of Things (IoT) systems. A review of specific features and challenges in the IoT systems impacting their security and reliability was conducted by Bures et al. [45]. Similarly, Mahmoud et al. [46] reviewed literature about the security concerns specific to IoT layers and devices by implementing corresponding countermeasures.

Humanoids generally combine hardware and software components from trusted supply chain entities. This trusted relationship introduces another element of a possible attack surface. The public spaces where these social robots will operate are dynamic (subject to human and environmental interference), thereby introducing the possibility of several physical attacks such as theft, vandalism, and sabotage. There is also the risk of physical harm to users during interaction due to cyber-attacks or malfunction [47]. If a humanoid is under the control of a malicious actor, it can result in a terrorist attack [48].

Unlike their other autonomous counterparts, autonomous vehicles (AVs) and unmanned aerial vehicles (UAVs) with relatively high operational speeds, social robots will operate at relatively low speeds or in stationary positions in some cases. This feature also introduces the humanoids to passive attacks like reconnaissance and non-invasive attacks like spoofing, jamming, blinding, and so on [49]. Other potential sources of attacks on social humanoids include the human element [50] and the AI system [51]. In this context, a current challenge is inadequate knowledge of the threat actors, attack surface, and threat landscape for social robots in public spaces. There is also a need for organizations and other stakeholders to understand potential attack scenarios so they can analyze and manage the risks associated with social robots as a business endeavor. Therefore, identifying potential threats and analyzing their impacts is crucial to any business continuity plan and mandatory to avoid regulatory sanctions.

The need for security, safety, privacy, and ethical consideration of social robots in public spaces has been discussed in previous works [25,52] without a framework for its implementation. Previous literature reviews provided a definition of social robots and their general application domains [23,53,54]. Other studies highlighted the potential applications of social robots in specific fields such as education [10,55–57], language studies [14–17], healthy ageing [58], elderly care [2,3], and mental health [6]. Moreover, other studies have established cybersecurity threat actors [48,59] and the AI threat landscape [51,60], but not in the context of social robots in public spaces whose threats exceed cybersecurity concerns. For example, Giaretta et al. [61] conducted a structured security assessment on Pepper in a laboratory without considering the particular aspects of public space. To the best of our knowledge, this is the first literature review on threat actors, attack surface, and threat landscape of social robots in public spaces.

The main contributions of this review are as follows:

1. A transdisciplinary perspective of threat actors, threat landscape, and attack surface of social robots in public spaces.
2. A set of comprehensive taxonomies for threat actors and threat landscape.
3. A comprehensive attack surface for social robots in public spaces.

4. A description of four potential attack scenarios for stakeholders in the field of social robots in public spaces.

The relevance of this study is threefold: (i) it discusses the security and privacy concerns of using social robots in public spaces, (ii) it provides guidance on risk assessment and management of social robots in public space, and (iii) it highlights current development and new research directions for social robots in public spaces.

The remainder of this paper is as follows. Section 2 presents background and related works. Section 3 presents the methodology adopted for this study. Section 4 contains the results obtained. Section 5 is for discussion, including limitations, threats to validity, and recommendations for future research. Section 6 presents two taxonomies, threat actors and threat landscape, while Section 7 concludes the paper.

2. Background and Related Works

This section introduces concepts and definitions used in this study. The first subsection introduces social robots, social robot sensors, public space, assets, vulnerabilities, threats, threat landscape, attacks, and attack surface. The second subsection presents some related works.

2.1. Key Concepts and Definitions

We briefly present some background concepts like the definition of social robots, public space, assets, vulnerabilities, threats, threat landscape, attacks, attack surface, cybersecurity, safety, and privacy.

2.1.1. Social Robots and Their Sensors

There are several definitions of social robots in previous works. Sarrica et al. [53] summarized five essential properties of social robots after reviewing 143 scientific publications and online definitions of the term "social robot" published from 2009 to 2015. The properties are (i) autonomy, (ii) physical embodiment, (iii) ability to sense and humanly respond to environmental cues, (iv) ability to interact with humans and other robots, and (v) ability to understand and follow social norms (rules). Essentially, a social robot must have a physical embodiment (anthropomorphic or non-anthropomorphic) that can autonomously navigate and interact with humans (not through scripting).

Another indispensable feature is the ability to interact with humans emotionally and socially while complying with acceptable social norms. According to Srinivas Aditya et al. [62], the fundamental features are perception, cognition, efficiency, interaction, and ethics. At the basic design level, a social robot receives signals from the environment (public space) through its sensors and responds through its actuators [63]. These sensors can be internal or external (environmental). Internal sensors help maintain the internal dynamics and stability of the robot. External sensors are responsible for perceiving the environment; they handle tasks such as vision, detection, range measurement, position measurement, tactile measurement, localization, and navigation of the public space (environment). Since sensors are the gateway to social humanoids, they represent a potential surface of attacks (see a list of typical sensors of social robots in Table A1 of Appendix A [64]). For a social humanoid to be intelligent in a human-like way during an interaction, it must possess sensors that emulate those of humans [64]. An AI system processes the data collected by these sensors before the social robot can understand and decide what type of response to give. Data collection is indispensable in social humanoids' operation; however, some of the collected data may be sensitive. Social humanoids collect a massive amount of data while interacting with the environment. Due to size and battery constraints, most of the computation, storage, and AI operations take place in the edge/cloud through a wireless communication link.

2.1.2. Public Space

In this study, public space is a publicly or privately owned space, an inside or outside place, that is accessible to all people, regardless of gender, race, ethnicity, age, or socio-economic level [23,65]. Access to these locations may be within certain hours of the day (as in the case of shopping malls, hospitals, elderly care homes, museums, etc.). Laws, culture, and institutional values strongly regulate public space; hence, appropriate behaviors and activities are expected in public spaces [66]. Social robots operating in public spaces are under little or no supervision; as such, users of the public space can have physical access to them. These locations are subject to natural (environmental) and human factors, which are dynamic and unpredictable. As people attribute values to a place from experience and interaction quality in such locations [67], social robots must comply with societal norms and behave as expected when operating in public spaces.

2.1.3. Assets and Vulnerabilities

According to NIST SP 800-160 [68], assets are significant applications, general support systems, high-impact programs, physical facilities, mission-critical systems, a team of people, a piece of machinery, or logically connected sets of systems. Assets include anything valuable for achieving company goals, which might be tangible (for example, a piece of hardware, software, firmware, a computer platform, a network device, or other technological components) or intangible (e.g., information, data, trademark, copyright, patent, intellectual property, image, or reputation). From the above definition, the assets of social robots in public spaces could include hardware, software, communication, cloud services, AI services, humans, and supply chains.

Vulnerabilities are "weaknesses or flaws in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" [69]. They can also be viewed as security exposures, bugs, deficiencies, or errors in any of the components stated above.

Threat actors would use attack vectors to exploit vulnerabilities in the social robots. Therefore, the MITRE Common Attack Pattern Enumeration and Classification (CAPEC) [70] attack domain could be used to classify the asset groups. The groups are software, hardware, communication, supply chain, human, cloud, and AI categories. This classification is consistent with a recent review on robotics cybersecurity conducted by Yaacoub et al. [71]. Social robots' software components consist of the operating system (ROS) and applications (e.g., gazebo) [72]. Their hardware component includes social robots' sensors, actuators, electronic control units (ECU), torso (body and arms), microcontroller/firmware, and battery [73]. Supply chain components overlap all other elements that incorporate the trusted entities involved in their manufacture, procurement, and use. The communication component includes communication devices and protocols of the social robot [44]. The human component includes users, end users, and other non-users (bystanders, passers-by, children, elderly, and the disabled) within the immediate vicinity of the social robot. Other stakeholders include not only the crew members of the supply team, such as hardware, software, cloud, AI, and communication, but also social robot business owners and regulators; finally, cloud and AI services are necessary for the social robot's storage, computation, and cognitive intelligence [51].

2.1.4. Threats and Threat Landscape

A threat is "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and or denial of service", according to the National Institute of Standards and Technology (NIST) [74]. Moreover, the European Union Agency for Cybersecurity (ENISA) [75] poses that "a threat landscape is a collection of threats in a particular domain or context, with information on identified vulnerable assets, threats, risks, threat actors and observed trends".

The term threat landscape has traditionally been associated with cybersecurity threats. Moreover, a particular domain or context, like social robots in public spaces, calls for a transdisciplinary approach, as suggested by Dautenhahn et al. [76] and Baxter et al. [77]. Dautenhahn et al. emphasized that social robot researchers need to view Human Robot Interaction (HRI) as not just an extension of previous efforts of one field, as there are unique differences that deserve special consideration. Baxter et al. brought the research community's attention to assumptions and technique bias introduced by each discipline (cognitive science, social science, AI, computer science, HCI, psychology, engineering, and robotics), resulting in differences in methods, difficulty in reproducing results, and low use of comparable measures among researchers. Similarly, Fortunati et al. [66] proposed that social robots in public space consist of three vital elements, social robots, humans, and the environment, using the triadic model proposed by Höflich [78]. According to Höflich, social robot interaction involves both a relationship and communication via a medium (social robots), where the medium is both a thing and an entity. The author referred to this as the ego–alter–robot triadic relationship. Therefore, the threat landscape for social robots in public spaces should consider both cybersecurity threats and physical, social, and public space threats.

Mayoral-Vilches [79] proposed two broad groups of threat direction for social robots: (i) threats directed to social robots by the environment (public space to a social robot—PS2SR) and (ii) threats directed to the environment by social robots (social robots to the public space—SR2PS). The first group (PS2SR) are threats directed to social robots by the environment (humans, properties, and public space—nature), while the second group addresses security threats of social robots to the immediate environment like property damage, threats to human privacy, and social norm violations.

Finally, cybersecurity threats can be classified using the Common Attack Pattern Enumerations and Classification (CAPEC) framework proposed by MITRE [70]. It proposes a taxonomy that includes software, hardware, communication, supply chain, social engineering, and physical attacks. In a recent work by Mavroeidis et al. [59], the motives for an attack may include taking (or stealing), copying (or reading), denying, deleting, damaging, or modifying data, while the outcome could be in the form of financial gain, business or technical advantage, sabotage, damage, or embarrassment.

2.1.5. Attacks and Attack Surface

According to NIST SP 800-12, Revision 1 [80], an attack is "any malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Or an attempt to gain unauthorized access to system services, resources, or information or an attempt to compromise system integrity, availability, or confidentiality". Threat actors exploit vulnerabilities during attacks. Attacks may be passive or active. In passive attacks, the attackers aim to acquire information about the targeted system (reconnaissance) without causing any damage or disruption [81]. On the contrary, active attacks can cause damage or disruption to an information system [82].

An attack surface is the set of points around the perimeter of a social robot component or its environment where an attacker could attempt to break in, disrupt, or steal data from the system, component, or environment [83]. From a cybersecurity perspective, the attack surface is viewed as physical (tangible) and digital (cyber) surfaces. The attack vectors of a system can also give valuable information about its attack surface.

2.1.6. Cybersecurity, Safety, and Privacy

Cybersecurity, safety, and privacy are three interwoven terms associated with the threat landscape of social robots in public spaces. A social robot cannot satisfy one of these terms without either of the other two [34]. A brief definition of those terms is presented below.

The UK National Cyber Security Strategy 2016–2021 [84] defines cybersecurity as "the protection of information systems (hardware, software and associated infrastructure), the

data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system or accidentally as a result of failing to follow security procedures".

NIST SP 800-160 [85] defines safety as "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment". Moreover, EN ISO 13482:2014 specifies the safety requirements for personal care robots, which also applies to social robots in public spaces. Physical harm prevention alone does not address the psychological harm that social robots can inflict on users during interactions [86]. From a holistic perspective, the safety of social robots in public spaces entails both the physical and psychological safety of users and the freedom of social robots from abuse, sabotage, theft, and destruction.

NIST IR 8053 [87] defines privacy as "freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual". There are currently no standards for privacy requirements for social robots in public spaces [37].

2.2. Related Works

To the best of our knowledge, this is the first review addressing the threat landscape of social robots in public spaces from a transdisciplinary perspective. However, for completeness, some related studies are briefly presented in the following subsections.

2.2.1. Cybersecurity Threat Actors

Timothy Casey developed the first comprehensive public threat actor library (TAL) for Intel Corporation in 2007 [88]. The list consists of eight attributes—intent, access, outcome, limit, resources, skill level, objectives, and visibility—thirty-two sub-attributes, and twenty-one threat actors. In 2021, the TAL was revised and improved to infer threat actors' types and characteristics [59]. Although the TAL provides valuable insights into understanding threat actors, its classification is too broad for social robots in a public space. Sailio et al. [48] identified eight threat actors for factories of the future by reviewing 22 different international cybersecurity reports. None of these reports identified the unique threats from the supply chain and public space peculiar to social robots. Yaacoub et al. [71] identified three robotics threat sources—malicious users, manufacturers/integrators, and external adversaries—and ten threat actors without mentioning their information source. This study is also focused on general robotics; hence, they did not address aspects of supply chain and environmental threat actors.

2.2.2. Safety and Social Errors in HRI

Lasota et al. [86] highlighted four approaches to safe human–robot interactions: (i) pre- and post-collision control methods, (ii) motion planning for human and non-human constraints, (iii) prediction of human activities, motion, and other robots' actions, and (iv) social robots' behavior adaptation to psychological factors. Moreover, Zacharaki et al. [89] classified studies on safe HRI to minimize risk into six categories: (i) perception, (ii) cognition, (iii) action, (iv) hardware features, (v) societal and psychological factors, and (vi) risk assessment through hazard analysis techniques. These studies focused on safety without consideration for other aspects of the threat landscapes of social robots, such as social norm violations and cybersecurity threats.

Tian et al. [90] proposed a taxonomy of social threats (errors) in HRI, focusing on performance and social norm violation errors. Authors emphasized the need for social-affective competence in terms of emotion and social skills during social interactions. Similarly, Honig et al. [91] reviewed failures in HRI, including technical and interaction-related failures. Interaction failures could be social norm violations, human errors, and environmental agent failure. The ability of social robots to interact in a socially acceptable manner is a significant factor influencing the acceptance and deployment of this new technology.

2.2.3. Social Robot Security

Mayoral-Vilches [79] reviewed the status of robot cybersecurity based on recent literature, questionnaires on robotic forums, and recent research results. Findings revealed that robotics defense mechanisms are complex and still in the early stages (immature), in most cases not covering the complete threat landscape and highly costly to implement. Moreover, Mayoral-Vilches concluded that practitioners in social robotics are mostly yet to observe cyber-attacks and recommended that future research should focus on zero-trust security approaches. Yaacoub et al. [71] reviewed the security of robots in general from the perspective of vulnerabilities and attacks. As a result, elements of robots' threat landscape were identified; however, this review lacks a well-defined methodology and does not discuss the context of public space. The elements identified include threat actors, the motive for attack, vulnerabilities, different types of attack, and their mitigations. Likewise, Cornelius et al. [92] surveyed mobile service robot threats, attacks, and defense mechanisms. In 2017, Cerrudo and Apa [93] published a white paper that identified hardware, software, and communication threats to social robots in laboratory settings. However, none of these previous studies addressed the threat landscape of social robots in public spaces considering all the actors.

2.2.4. Cybersecurity Threat Landscape

ENISA [94] is an international body responsible for the annual publication of the cybersecurity threat landscape since 2013. The threat landscape usually contains cyber threat intelligence with a specific sectorial taxonomy using an established methodology [95]. We could not find any existing threat landscape for social robots in public spaces. In 2011, Kim-Kwang Choo [96] mentioned that routine activity theory could reduce the occurrence of cyber threats. In collaboration with the Berkman Klein Center for Internet and Society of Harvard University, Microsoft Corporation proposed a threat taxonomy for AI security [60]. The proposed taxonomy can be applied to AI services of social robots in public spaces.

2.2.5. Summary of Related Works

To sum up, the complete threat landscape and attack surface of social robots in public spaces has received little attention so far. Most studies on threat actors, safety, social errors, robot security, and threat landscape investigated general robotics security without considering the peculiarity of social robots in public spaces. This review seeks to address the topic from the following perspectives:

(i) The public space in which social robots will operate is dynamic and subject to various human and natural factors.
(ii) Social robots will operate with little or no supervision and very close to users (including threat actors), which will increase the probability of attack success.
(iii) The enabling communication technologies for social robots in public spaces are heterogeneous, which further increases their attack surface, as the whole system is more complicated than the sum of its constituent parts.
(iv) The definition of the threat landscape for social robots in public spaces should include the perspective of all stakeholders and not just the cybersecurity discipline.

3. Methodology

The methodology adopted for this study follows the guidelines by Kitchenham and Charters [97] for conducting a systematic literature review (SLR) in software engineering. According to the guidelines, the review process includes three stages: planning the review, followed by conducting the review and reporting the study. Figure 1 provides an overview of this study's research methodology.

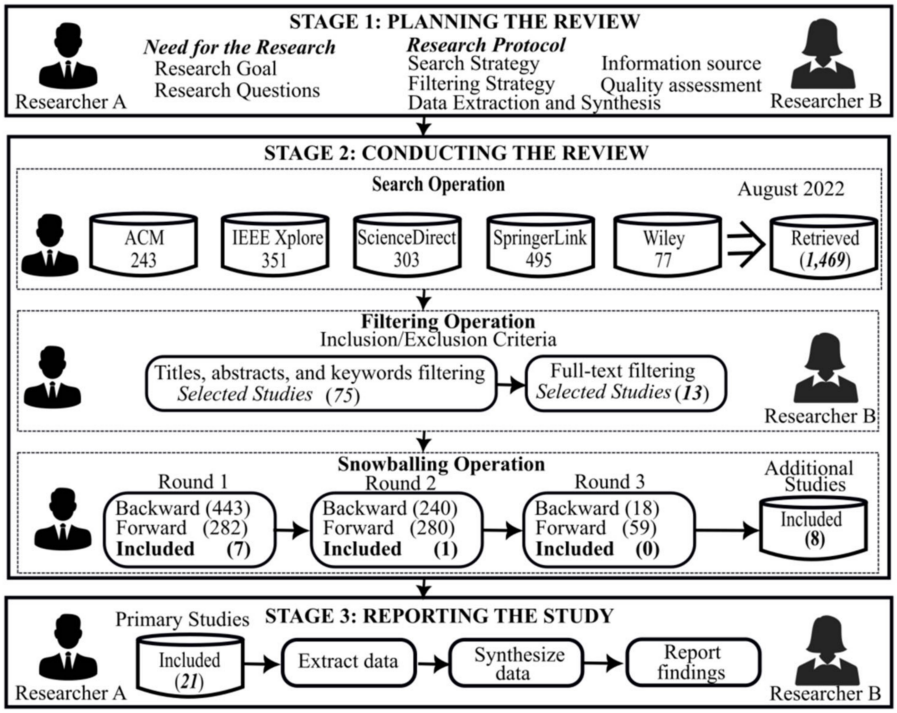


Figure 1. Overview of the research process for this study.

3.1. Planning the Review

According to the guidelines by Kitchenham and Charters [97], the two primary tasks of the planning stage are determining the research needs and creating a research protocol. In determining the need for the study, we clearly state the research goals, objectives, and research questions. A research protocol was also defined to provide a set of complete instructions on how to conduct the study; specifically, the information source, the search and filtering strategies, the quality assessment, and data extraction strategies, and how to report the results. The following subsection will provide more details of the planning stage activities.

3.1.1. The Need for the Study

A brief description of this study's research goal, objectives, and research questions are as follows.

Research goal and objectives. This review aims to systematically review and synthesize empirical research on the threat landscape of social robots operating in public spaces. The primary objective in this study is divided into four sub-objectives: (i) we would like to investigate and report the trend of empirical research in this field; (ii) we also like to identify and report the potential threat actors and their motivation for attacks in this domain; (iii) we want to explore and document social robots' assets, threats, and vulnerabilities in public spaces; finally, (iv) we would like to identify and enumerate attack surfaces for social robots in public spaces.

Research questions are based on the research objectives, and we formulated the following research questions (RQs) in four groups.

Group 1: Research trend of social robots in public spaces

- RQ1.1: What is the research trend of empirical studies on social robots in public spaces?
- RQ1.2: What is the citation landscape of the primary studies in this area?
- RQ1.3: What are the reported research methods for these empirical studies?

Contribution: Knowing the research focus, types, trends, and publication sources for social robots in public spaces will give the practitioners and the research community a

high-level overview of the research landscape. In addition, the research trend can also review essential studies in this emerging field

Group 2: Threat actors and their motives for attack

- RQ2.1: Who are the reported potential threat actors for social robots in public spaces?
- RQ2.2: What are the reported threat actors' motives for attack?

Contribution: Knowing the reported threat actors and their motives, especially those related to social robots, will enhance the development of machine-readable solutions to mitigate such attacks.

Group 3: Identifying assets, threats, and vulnerabilities

- RQ3.1: What are the reported assets (sub-components) of social robots in public spaces?
- RQ3.2: What are the reported threats?
- RQ3.3: What are the reported vulnerabilities?

Contribution: Answering these questions will provide valuable insights for security practitioners, hardware manufacturers, and social robot business owners during risk analysis and management.

Group 4: Attack surface of social robots in public spaces

- RQ4.1: What are the reported attacks on social robots in public spaces?
- RQ4.2: What are the reported attack scenarios?
- RQ4.3: What are the reported attack impacts?
- RQ4.4: What are the reported attack mitigations?

Contribution: Knowing the reported attack surface before operating social robots in public spaces is valuable. Social robot researchers, designers, developers, practitioners, and business owners will benefit from such knowledge.

3.1.2. Developing and Evaluating the Research Protocol

We developed and validated a research protocol for the study during the planning stage. The research protocol contains guidelines on the information source, search and filtering strategies, quality assessment, and data extraction/synthesis strategies. In what follows, we briefly describe our research protocol.

Information source. We included five scientific digital libraries for searching the primary studies included in this review. These databases are considered the top academic search engines for computer science, software engineering, and IT security SLR studies, e.g., [98]. They are also suggested by Kitchenham and Charters [97]. The digital libraries consulted are ACM digital library, IEEE Xplore, ScienceDirect, SpringerLink, and Wiley online library (details are available in the study's Supplementary Materials [99]).

Search strategy. Given the nature of this review, we chose specific keywords to focus our search on the studies that were most relevant to the topic. The five keywords are "social robot", "social humanoid", "threat", "attack", and "vulnerability". We also included a single inflected variation of each term, "social robots", "social humanoids", "threats", "attacks", and "vulnerabilities". The first two terms (social robot and humanoid) will ensure that our search results will have only studies relating to socially interactive robots [100]. The last three terms (threat, attack, and vulnerabilities) will ensure that our search results only include studies focusing on the threat landscape, attack surface, and threat actors of such socially interactive robots. We chose these keywords after conducting trial searches with other keywords such as "companion robots", "sentient robots", and "public space robots". We identified two related studies during the preliminary searches [61,101], which were used for testing the results of our final search string.

To ensure consistency of our search results across all five digital libraries, we constructed a search string, ("social robot" OR "social robots" OR "social humanoid" OR "social humanoids") AND ("attacks" OR "attack" OR "threat" OR "threats" OR "vulnerability" OR "vulnerabilities"), for the search process. We searched all digital libraries on the 2nd of August 2022, filtering the search results from January 2010 to December 2021. We began in

2010 because, according to Google Ngram Viewer (https://books.google.com/ngrams/, accessed 2 August 2022), that month saw a notable increase in the number of publications on social robots. Although some relevant studies before January 2010 could be missing, our primary focus is on the current research in this area, and ten years provide a good timeframe due to the rapid pace of technological advancement in this field.

Filtering strategy. The guidelines [97] specify that a list of inclusion and exclusion criteria should be prepared to aid the filtering of search results. Therefore, we generated the following inclusion and exclusion criteria:

Inclusion criteria include four items:

1. **Domain (I1)**: The main field must be socially interactive robots in public spaces. The study must explicitly discuss threats, attacks, or vulnerabilities of social robots/humanoids. Public space in this context refers to any location, indoor or outdoor, accessible to the members of the public. Access to these public locations is the key to our usage of public space in this study, not ownership. Also considered as public spaces for this study are smart homes for elderly care, museums, playgrounds, libraries, medical centers, or rehabilitation homes that may not be easily accessible to all members of the public but allows visitors periodically.
2. **Methods (I2)**: Empirical studies using quantitative, qualitative, or mixed methodologies. Such studies could be an interview, case studies, or experiments which were observed in the field, laboratory, or public settings. We focused on empirical studies to ensure that our findings were backed with empirical evidence, not philosophical opinions.
3. **Type (I3)**: Study types were to include journal articles, conference papers, book chapters, or magazine articles. These studies must be peer-reviewed.
4. **Language (I4)**: English language only.

Exclusion criteria include eight items (E1–E8).

1. **Irrelevant studies (E1):** Studies outside the specified domain above. We also classified non-empirical studies that are related to the above domain as irrelevant to this research.
2. **Secondary studies (E2)*:*** All secondary studies in the form of reviews, surveys, and SLRs.
3. **Language (E3):** Studies that are not in the English language.
4. **Duplicate studies (E4):** Studies duplicated in more than one digital library or extended papers.
5. **Inaccessible studies (E5)*:*** All studies with access restrictions.
6. **Short papers (E6):** Work-in-progress and doctoral symposium presentations that are less than four papers.
7. **Front and back matter (E7):** Search results containing all front matter like abstract pages, title pages, table of contents, and so on; we also excluded all back matter like index, bibliography, etc.
8. **Papers that are not peer-reviewed (E8):** All studies that did not undergo peer review during snowballing.

Quality assessment strategy. We adopted the quality assessment strategy recommendation of Kitchenham and Charters [97], focusing on the design, conduct, analysis, and conclusion of the primary studies. The quality of the studies was ranked on a scale of 0 to 1 (No = 0, Partially = 0.5, Yes = 1). The quality assessment questions used for this study are available online [99]. The total quality assessment score was a percentage, with 50% being the least acceptable quality assessment score. We evaluated the quality of the papers throughout the filtering and data extraction stage of this SLR.

Data extraction and synthesis. We developed a data extraction checklist (more details are available online [99]) to aid the extraction of relevant data from the primary studies. There are 24 fields in the list. In the first 13 fields (1–13), we extract data relating to the RQs of group 1; the next two fields addressed group 2 RQs. Similarly, records 14–20

extracted data addressing RQs of group 3, while in the last four fields (21–24), we extracted information for group 4 RQs. In analyzing the research trends in this field, we intend to extract information about the authors' affiliations (sectors and countries). The sector refers to academia, industry, or mixed, while the country is the country affiliation of the authors. We also extracted data on the impacts of attacks based on the core security objectives of confidentiality (disclosure), integrity (alteration), availability (destruction), and privacy (privacy violation).

Evaluating the research protocol. The research protocol for this study was developed based on well-known software engineering literature review guidelines, and two expert researchers reviewed it. As input assessment and improvements were incorporated into the final version, two authors conducted preliminary searches and testing utilizing the research protocol. Before the review process started, meetings were held to discuss and address all concerns and issues.

3.2. Conducting the Review

The four primary review activities include searching, filtering, snowballing, and quality assessment. We present a brief description of each exercise in the following subsections.

3.2.1. Searching

The first author (Researcher A) conducted the search process in August 2022, while an experienced researcher (Researcher B) validated the results. The search operation was performed using the research protocol search string and information source. For easy reproducibility, we provide the URL links of the obtained results [99]. The data were first extracted from the bibliographic databases using a reference manager (Zotero (https://www.zotero.org/, version 6.0.9, accessed 2 August 2022)) and later exported in CSV (Comma Separated Values) format to a spreadsheet application (Microsoft Excel template). The search results obtained are presented in Table 1.

Table 1. Summary of Search results and excluded studies.

Database	Search	E1	E2	E3	E4	E5	E7	First Round
ACM Digital Library	243	191	10		1	11	17	13
IEEE Xplore	351	236	26		16		50	23
ScienceDirect	303	251	29	1		1	13	8
SpringerLink	495	353	101	1	1		13	26
Wiley Online Library	77	49	7		1		16	4
Total	1469	1080	173	2	19	12	109	74

3.2.2. Filtering

The filtering process was conducted in two rounds, using the inclusion and exclusion criteria specified in the study's research protocol. We assigned exclusion codes (E1–E8) to justify the reason for excluding any paper.

The first step in the filtering operation was removing duplicate studies based on titles and abstracts. Duplicate studies are studies that appeared as unique records more than once. This was easily implemented in our spreadsheet template using conditional formatting. The first occurrence of a duplicate study was retained, while the others were excluded. The duplicate studies were mainly from past ACM/IEEE international conferences on human–robot interactions. We found 19 duplicate studies (exclusion code E4). Next, 109 studies were excluded, as they contained front matter and back matter like title pages, table of contents, abstracts, indexes, posters, list of tables, etc. (exclusion code E7). Moreover, 173 studies were excluded as secondary studies (exclusion code E2). Two studies written in other languages were also excluded (exclusion code E3). Exclusion code E1 is for irrelevant studies, which amounted to 1080, as shown Table 1. Irrelevant studies are those papers that could not provide answers to our research questions, or their application settings are

outside the scope of this study. This first filtering round involves reading each paper's title, keywords, and abstracts to assess if the study was irrelevant. At the end of the first round, 74 studies were included for full-text filtering, while we excluded 1395 studies, as shown in Table 1.

The second round of the filtering operation involves full-text reading and a quality assessment of the papers. We examined the included 74 studies using the full text to ascertain if the study could answer any of our research questions. At the end of the second round, only 13 papers met our inclusion criteria as primary studies. These included studies were assigned a unique identifier number (PS01–PS13) for easy reference.

3.2.3. Snowballing

As specified in the guidelines [97], we screened the references and citations of the included 13 studies for any additional relevant papers. This process is known as backward and forward snowballing [102]. In backward snowballing, we used the reference list of the included 13 papers from the publisher's website. In forward snowballing, we consulted their citations on Google Scholar (31 August 2022). The snowballing included three rounds. In the first round, we examined 443 references and 282 citations of all 13 included studies using our selection (inclusion/exclusion) and quality assessment criteria. We found seven additional papers relevant to our study from the first round. We assigned a unique identifier for these seven papers (PSA01–PSA07). In the second round of snowballing, we examined 240 references and 280 citations of the seven papers included in the first round. The second round produced one paper (PSB01). In the final round, we examined the 18 references and 59 citations of PSB01 and found no study that met our inclusion/quality assessment criteria (see details of snowballing summary in Table A2 of Appendix B). As a result, an additional eight studies were identified as relevant, making for 21 total primary studies.

3.2.4. Quality Assessment

We assessed the quality of our primary studies based on the empirical research design, conduct, data analysis and research conclusions drawn from the studies. Four quality assessment questions assessed the design in terms of research aim, adequate measurement of threats, clear definition of research measures, and authors' introduction of bias during the study. Three questions each assessed the conduct of the empirical research and its data analysis. Finally, five questions considered the conclusions drawn from each empirical study. The score assigned to each study is based on authors' assessment of each paper. The assessment score ranges from 70–93.3% (see details of quality assessment score in Table A3 of Appendix C). The results revealed that our primary studies are of good quality.

3.2.5. Data Extraction and Synthesis

We extracted relevant data from our primary studies to respond to our RQs. Each set of extracted records consists of the following information: study ID, RQ, data, type of data, and quotes. For instance, the second record on the extracted data reads as follows: PS01; 1.1; Robot under study; Pepper; "In this paper, we perform a thorough security assessment over Pepper, a commercial human-shaped social robot by SoftBank Robotics". In this case, the study ID is PS01, the research question (RQ) is 1.1, the data extracted is on the robot under study, while its type is Pepper, and the quotation stated was taken directly from the full text. If a study reported more than one data type, another record was created to capture it. For instance, there are six threat actor data records for PS01 because the study reported six different types of threat actors (details are available online [99]).

4. Results

The first observation is that out of the 1469 papers retrieved using the search string, only 21 empirical studies could answer at least one or more of our proposed research questions in the domain of social robots in public spaces. The findings of our SLR are presented below according to the RQ groups.

4.1. Research Trends for Social Robots in Public Spaces

4.1.1. What Is the Research Trend of Empirical Studies on Social Robots in Public Spaces?

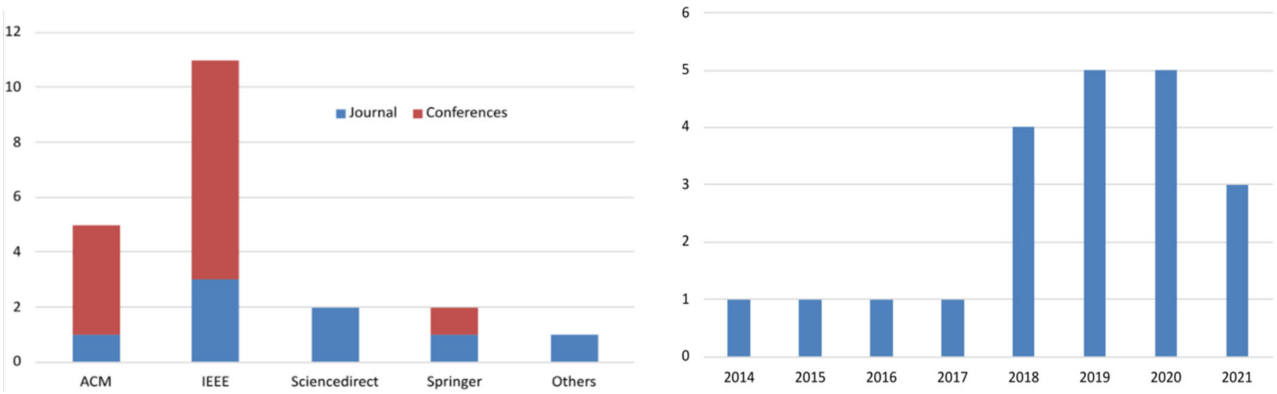
Our twenty-one primary studies consist of eight journal publications and thirteen conference proceedings. A complete list of all primary studies showing authors, year of publication, and titles is presented in Table 2.

Table 2. Summary of primary studies.

#	IDs	Ref.	Authors	Year	Title	C*	AvgC^
1	PSA02	[103]	Brščić, Dražen; Kidokoro, Hiroyuki; Suehiro, Yoshitaka; Kanda, Takayuki	2015	Escaping from Children's Abuse of Social Robots	169	24
2	PS12	[104]	Lin, Jiacheng; Li, Yang; Yang, Guanci	2021	FPGAN: Face de-identification method with generative adversarial networks for social robots	61	61
3	PS09	[105]	Zhang, Yin; Qian, Yongfeng; Wu, Di; Hossain, M. Shamim; Ghoneim, Ahmed; Chen, Min	2019	Emotion-aware multimedia systems security	57	19
4	PSA05	[106]	Aroyo, Alexander Mois; Rea, Francesco; Sandini, Giulio; Sciutti, Alessandra	2018	Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble?	57	14
5	PS02	[107]	Tan, Xiang Zhi; Vázquez, Marynel; Carter, Elizabeth J.; Morales, Cecilia G.; Steinfeld, Aaron	2018	Inducing Bystander Interventions During Robot Abuse with Social Mechanisms	50	13
6	PS01	[61]	Giaretta, Alberto; De Donno, Michele; Dragoni, Nicola	2018	Adding salt to Pepper: A structured security assessment over a humanoid robot	34	9
7	PSA06	[108]	Yang, Guanci; Yang, Jing; Sheng, Weihua; Junior, Francisco Erivaldo Fernandes; Li, Shaobo	2018	Convolutional Neural Network-Based Embarrassing Situation Detection under Camera for Social Robot in Smart Homes	34	9
8	PS07	[109]	Fernandes, Francisco Erivaldo; Yang, Guanci; Do, Ha Manh; Sheng, Weihua	2016	Detection of privacy-sensitive situations for social robots in smart homes	31	5
9	PSA03	[110]	Bhardwaj, Akashdeep; Avasthi, Vinay; Goundar, Sam	2019	Cyber security attacks on robotic platforms	16	5
10	PS08	[111]	Truong, Xuan-Tung; Yoong, Voo Nyuk; Ngo, Trung-Dung	2014	Dynamic social zone for human safety in human-robot shared workspaces	14	2
11	PS05	[112]	Krupp, Margaret M.; Rueben, Matthew; Grimm, Cindy M.; Smart, William D.	2017	A focus group study of privacy concerns about telepresence robots	11	2
12	PSB01	[113]	Yamada, Sachie; Kanda, Takayuki; Tomita, Kanako	2020	An Escalating Model of Children's Robot Abuse	11	6
13	PS04	[114]	Olivato, Matteo; Cotugno, Omar; Brigato, Lorenzo; Bloisi, Domenico; Farinelli, Alessandro; Iocchi, Luca	2019	A comparative analysis of the use of autoencoders for robot security anomaly detection	5	2
14	PS10	[115]	Vulpe, Alexandru; Paikan, Ali; Craciunescu, Razvan; Ziafati, Pouyan; Kyriazakos, Sofoklis; Hemmer, Adrien; Badonnel, Remi	2019	IoT Security Approaches in Social Robots for Ambient Assisted Living Scenarios	5	2
15	PS11	[116]	Abate, Andrea F.; Bisogni, Carmen; Cascone, Lucia; Castiglione, Aniello; Costabile, Gerardo; Mercuri, Ilenia	2020	Social Robot Interactions for Social Engineering: Opportunities and Open Issues	5	3
16	PSA01	[117]	Hochgeschwender, Nico; Cornelius, Gary; Voos, Holger	2019	Arguing Security of Autonomous Robots	4	1
17	PS03	[118]	Joosse, Michiel; Lohse, Manja; Berkel, Niels Van; Sardar, Aziez; Evers, Vanessa	2021	Making Appearances: How Robots Should Approach People	3	3
18	PS06	[119]	Vasylkovskyi, Viktor; Guerreiro, Sérgio; Sequeira, João Silva	2020	BlockRobot: Increasing privacy in human robot interaction by using blockchain	3	2
19	PS13	[101]	Mazzeo, Giovanni; Staffa, Mariacarla	2020	TROS: Protecting Humanoids ROS from Privileged Attackers	2	1
20	PSA07	[120]	Sanoubari, Elaheh; Young, James; Houston, Andrew; Dautenhahn, Kerstin	2021	Can Robots Be Bullied? A Crowdsourced Feasibility Study for Using Social Robots in Anti-Bullying Interventions	1	1
21	PSA04	[121]	Cui, Yuning; Sun, Yi; Luo, Jun; Huang, Yonghui; Zhou, Yuxuan; Li, Xuelei	2021	MMPD: A Novel Malicious PDF File Detector for Mobile Robots	0	0

C* = Citation as of 31 August 2022, Avg C^ = Average citation per year.

As expected, there are more conference proceedings than journal publications because conference proceedings are one of the most common ways of communicating research findings. Figure 2 shows the distribution of the number of studies by (a) databases and (b) publication year. IEEE Explore contributed the highest number of papers (52.4%), consisting of three journal publications and eight conference proceedings. ACM contributed five papers (23.8%), comprising one journal publication and four conference proceedings. ScienceDirect and SpringerLink contributed two studies each. During our snowballing operation, one journal publication was identified in another database (MDPI). These studies were published by authors from 18 different countries, with fifteen studies from academic research institutions, while six of them represent a collaboration between industry and academia. China has the highest number of empirical research studes (five), followed by the United States and Italy (four studies each), Denmark (three), and Japan and Luxembourg (two studies each). There are 12 other countries that contributed one report each, as presented in Table A4 of Appendix C. Figure 2b shows a growing interest in this research domain from 2018, which was possibly affected by the movement restriction of COVID-19 in 2020 and 2021.



(**a**) (**b**)

Figure 2. (**a**) Distribution of papers by database; (**b**) Distribution of papers by year.

Table 3 lists the social robots studied and their corresponding application domain. Pepper by Softbank Robotics is the most studied social robot with four occurrences, while Robovie2 and MAT social robots were studied in two papers each. Other social robots such as NAO, Atlas, Cozmo, ICub, Eddie Platform, and AIWAC were studied in one paper each. Two studies did not disclose the identity of the studied social robot for security reasons. Moreover, social robots were customized in four studies by using a separate camera and other sensors. The most studied application domains were health care (three) and shopping malls (three), followed by offices (two), museums (two), and smart homes (two). The remaining application domains were education (one), entertainment (one), and playground (one). General human–social robot interaction application scenarios were applied in five studies.

4.1.2. What Is the Citation Landscape of Studies on Social Robots in Public Spaces?

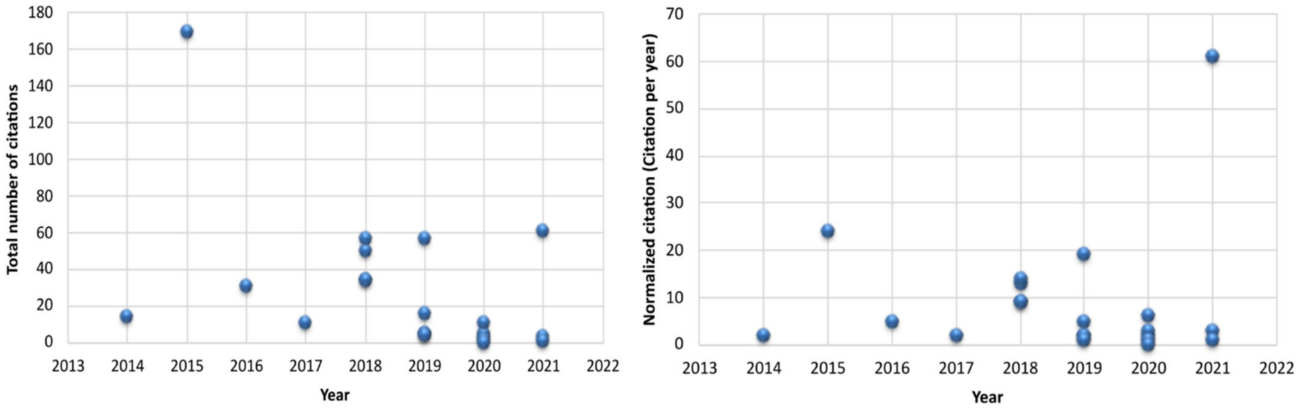
To understand the citation landscape of our primary studies, the citations were extracted from Google Scholar on 31 August 2022. The citation landscape was determined by absolute citation and normalized citation per year, as suggested by Garousi and Fernandes [122]. Citation rank can help readers and new researchers to pinpoint the most influential research in a given field. It also gives an insight into our primary studies' impact (a measure of their quality). We provided this citation analysis as a guide and starting point for interested researchers in this field. Table 2 lists the absolute citation and normalized citation, and Figure 3a,b depicts the same information by year of publication. PSA02 is the most cited paper, while PS12 has the highest normalized citation rating. Only one study

(PSA04) published in 2020 had no citation yet when conducting this review. It suggests that studies in this domain are attracting interest.

Table 3. List of primary studies, application domain, and social robot type employed.

#	IDs	Application Domain	Social Robot
1	PS04	Education	Pepper
2	PS02	Entertainment	Cozmo
3	PS11	General Human–Social Robot Interaction	Pepper
4	PSA07	General Human–Social Robot Interaction	Atlas
5	PS12	General Human–Social Robot Interaction	MAT *
6	PS13	General Human–Social Robot Interaction	NAO
7	PSA03	General Human–Social Robot Interaction	Not Stated (for security reasons)
8	PS09	Health Care (Health monitoring system)	AIWAC
9	PS06	Health Care (Hospital)	Blockrobot *
10	PS10	Health Care (Personalized rehabilitation and coaching or ambient assisted living services)	QT Robot
11	PS05	Home, Work, and Public	PR-2 robot, Beam+ Telepresence robot, and ALICE (Roboceptionist Kiosk)
12	PS03	Museum	Nomad Scout
13	PSA01	Museum	Pepper
14	PS04	Office guide and Shopping Mall Assistant	Not Stated
15	PS08	Offices (Shared workplaces)	Eddie platform *
16	PSA05	Playground	Icub
17	PS01	Sales Stores	Pepper
18	PSA02	Shopping Mall	Robovie2
19	PSB01	Shopping Mall	Robovie2
20	PS07	Smart homes	ASCC Home Service Robot *
21	PSA06	Smart homes	MAT *

* Social robots customized by authors.



(**a**) (**b**)

Figure 3. Citation landscape of this study. (**a**) Absolute citation per paper; (**b**) Normalized citation per paper.

Figure 4 illustrates the average number of authors in this domain. As one can see, the number is four authors per study, which is consistent with the study conducted by Garousi and Fernandes [122].

4.1.3. What Research Methods Are Employed in Studies on Social Robots in Public Spaces?

Quantitative research is the dominant research methodology adopted in the empirical studies of social robots in public spaces (61.9%, PS01, PS03, PS04, PS06, PS07, PS08, PS09, PS12, PS13, PSA01, PSA03, PSA04, PSA06), followed by mixed research (28.6%, PS10, PS11,

PSA02, PSA05, PSA07, PSB01) and qualitative research (9.5%, PS02, PS05). The research approaches were experiments (nineteen), observation (six), surveys and questionnaires (four), use case (two), and one focus group (see details in Table A5 of Appendix C).

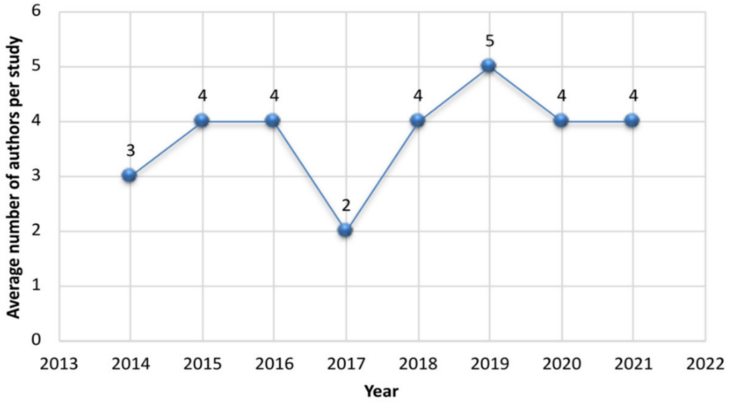


Figure 4. Average number of authors per year in the SLR domain.

4.2. Social Robot Threat Actors and Their Motives for Attack

This section reports the identified threat actors and their motives for the attack. Identifying threat actors and their motives for attacks is essential for detecting, preventing, and neutralizing any security threat.

4.2.1. Who Are the Reported Potential Threat Actors for Social Robots in Public Spaces?

Threat actors reported in the primary studies are classified as attackers (eleven), hackers (seven), thieves (five), and users (eight). PS13 reported four types of user-related threat actors (malicious, malevolent, root, and privileged user). Table 4 shows a description of each of these general threat actors (using the NIST (https://csrc.nist.gov/glossary?sortBy-lg=relevance&ipp-lg=100, accessed 20 August 2022) definition).

Table 4. General threat actor category commonly used in our primary studies.

Threat Actors	Description	IDs
Attacker	Anyone acting to compromise a social robot or to try to take advantage of a social robot's known vulnerabilities	PS04, PS07, PS09, PS10, PSA06
Hacker	Any unauthorized person who makes an attempt to access a social robot or successfully does so	PS01, PS04, PS05, PS10, PS13, PSA03, PSA04
Thief	Anyone who illegally obtains and utilizes another person's personal information or property, usually for economic advantage, through fraud or deception	PS01, PS04, PS05, PS13, PSA01, PSA03
User	A person or system process with access rights to a social robot	PS02, PS09, PS10, PS13, PSA06

Additionally, the classification proposed by Mavroeidis et al. [59] was used to group our identified threat actors based on access (internal and external), intent (intentional and non-intentional), and resources (individual, skill, groups, organization, and country). Internal threat actors could be employees (insiders—PS01, PS13, PSA03), users, or others (e.g., vendors as in PS06), while external actors could be competitors (PSA03), hackers, cyber criminals (PSA03), state actors (PSA01, PSA03), organized criminals (PS05, PSA03), and so on. An intentional actor could be an internal (e.g., disgruntled employee, as in PSA03) or external threat (PS13, PSA01). An unexpected finding was to identify children (PS02, PSA02, and PSA05) and social robots (PS03 and PS08) as threat actors. There are reports of children abusing social robots and social robots violating/invading users' privacy/preferences and social norms. Finally, based on the resources, there are individuals (PSA01), wannabes

(PSA03), trusted entities in the supply chain (PS06), non-government groups (PSA01), state-level intelligence (PSA01), nation states (PSA03), academic research groups (PSA01), and social engineers (PS11 and PSA05) (see details in Table A6 of Appendix D).

4.2.2. What Are the Reported Threat Actors' Motives for Attack?

Understanding threat actors' motives for attack allows effective security design against such threats. The reasons for cyber-attacks on social robots in public spaces differ for physical, social, and public-space-related attacks. In this review, seven motives were identified from an information security perspective: (i) gather information (reconnaissance), (ii) gain/escalate user privileges, (iii) modify data (users' or social robot's operation data), (iv) read (take or steal) data, (v) execute an unauthorized command, (vi) deny/disrupt services/operation, (vii) damage/destroy assets or properties. The outcome/effects of these attacks can be in the form of financial gain, reputational damage, business advantage, embarrassment to users or business owners, blackmail, technological edge, business sabotage, or property damage. It is sometimes difficult to differentiate the outcome from the motive, as the effect is what the threat actor wants. Information gathering (reconnaissance) is usually the first step in any cyber-attack [123]. The information gathered could be about the operation of the social robot or users' data (about 90%, i.e., 19 of 21 studies). Gaining and escalating privileges (PS01, PS09, PS10, and PS13) are primarily targeted at social robots' applications and software through various cyber-attacks. Modifying data was reported in five studies (PS01, PS09, PS13, PSA01, and PSA03), while reading (taking or stealing) data was reported in five studies (PS01, PS09, PS13, PSA01, and PSA03) (see details in Table A7 of Appendix D).

The reported motive for children's robot abuse was curiosity, fun, and imitating other children (PS02, PSA02, and PSB01). On physical attacks on humans by social robots, two studies (PS08, PS10) reported malfunction (resulting from design failure or cyber-attack) and inadequate cognitive/intelligent control systems of the social robot AI (PS10 and PS09). The last reason is also valid for violating social norms when a cyber-attack is not involved (usually due to poor social interaction design implementation of AI components).

The outcome/effects of an attack could be blackmail (PSA01, PSA03), individual/business reputational damage (PSA03, PS04), physical harm to humans, or property damage (PS04, PSA03). Industrial espionage may have a technical/business advantage as its motive (PSA03). Nation state actors may want economic damage or to use acquired information as a political weapon (PSA03, PSA01). Wannabes may want to show off their recently acquired talent for recognition (PSA03). Cyber criminals/thieves (sometimes including disgruntled employees) are strongly motivated by financial gains (PSA03). Competitors may be motivated by technical/business advantages (PSA03). Terrorists may be motivated by property damage or physical harm to humans because of a particular ideology (PS01, PS04).

4.3. Identifying Assets, Threats, and Vulnerabilities of Social Robots in Public Spaces

Identifying the valuable assets, their associated vulnerabilities, and the potential threat that a threat actor can exploit is vital in risk analysis and management of social robots in public places. This section presents reported assets, threats, and vulnerabilities.

4.3.1. What Are the Reported Assets (Sub-Components) of Social Robots in Public Spaces?

The asset classification is presented in Table 5. As expected, all primary studies reported hardware and human components. About 81% (seventeen) of the studies reported software components, while communication and cloud were reported by 38% (eight) and 33% (nine), respectively. Supply chain and AI were least represented, i.e., 19% (four) and 10% (two), respectively. However, a complete threat landscape should envisage threats that these essential components can pose to the system. Therefore, more research is needed to explore the practical role of AI and supply chain in this context.

Table 5. Asset categories reported in this study.

	Assets	PS01	PS02	PS03	PS04	PS05	PS06	PS07	PS08	PS09	PS10	PS11	PS12	PS13	PSA01	PSA02	PSA03	PSA04	PSA05	PSA06	PSA07	PSB01	Total (%)
1	Software	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			21
2	Hardware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	26
3	Communication	✓			✓		✓			✓	✓			✓	✓		✓						10
4	Human	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	26
5	Cloud	✓					✓			✓	✓			✓	✓		✓						9
6	AI	✓					✓			✓	✓												5
7	Supply chain										✓						✓						3

4.3.2. What Are the Reported Threats?

Two directions of threat were identified in this study: (i) threats directed to the public space by the social robot (SR2PS) and (ii) threats directed to the social robot by public space actors (PS2SR). The public space in this context refers to the following components: human and natural factors. Table 6 shows that about 86% (eighteen) of our primary studies reported threats from social robots to public space, compared to 29% (six papers) that reported threats from public space to social robots. Moreover, 14% (three) of these studies investigated the threats in both directions. It suggests that more research is needed to investigate social robots' directed threats in public spaces. The threat direction also reveals that more research exists on social robot threats to humans and public space than those protecting social robots from public space factors. Insights and research in the other threat direction could benefit investors, especially during risk assessment and management.

Table 6. Threat direction and categories.

Threat Direction	Threats Category *	IDs
PS2SR	P (robot abuse)	PSA02, PS02, PSB01
SR2PS	P (human safety)	SR2PS
	P (robot abuse)	PSA07
	S	PS03
	C/Ps/S (personal space and touch)	PS05
	C/S (nakedness)	PS07
	C	PS12, PSA04, PS06, PS10, PS09, PSA06
	C/S (trust violation)	PS11
	C/Social (trust exploitation)/Ps	PSA05
	C/P (human safety)/Ps	PSA01
	C/P (human safety)/Ps/S	PSA03
PS2SR and SR2PS	C	PS04
	C/P (human safety)	PS01, PS13

* C = Cybersecurity, S = Social, Ps = Public space.

The reported threats were also categorized into cybersecurity, physical, social, and public space by using MITRE CAPEC, i.e., software, hardware, communication, social engineering, physical, and supply chain.

Physical threats cover threats to human safety (possibly resulting from social robot failure and design flaws without cyber-attack) and threats directed at social robots (e.g., robot abuse, maltreatment, theft, vandalism, sabotage). This category differs from physical cybersecurity attacks that cover excavation, interception, reverse engineering, bypassing physical security, hardware integrity attack, physical hardware theft, and destruction [70].

Social threats surround threats associated with social robots not adhering to public space social norms. It considers the threat of property damage or natural factors such as fire, flood, weather/rain disrupting communication, war, and terrorism as public space threats.

Table 6 lists the primary studies and their related threats: cybersecurity 67% (fourteen), social 48% (ten), physical 29% (six), and public space 19% (four). Most studies reported more than one threat (PS01, PS05, PS07, PS11, PS13, PSA01, PSA03, PSA05). Although it is not surprising that most of the studies are focused on cybersecurity, other kinds of threats were also identified. It suggests that physical, social, and public space threats should also be considered because of their relevance in this domain.

4.3.3. What Are the Reported Vulnerabilities?

In this SLR, specific vulnerabilities (weaknesses or security policy violations) in existing social robot design and implementation were found. Table 7 presents a summary of the vulnerabilities reported in the primary studies. Some of these vulnerabilities may be well-known today; however, they were significant when reported (e.g., the use of a default username and password and insecure communication over HTTP in PS01).

Table 7. Vulnerabilities reported in the primary studies.

IDs	Category *	Vulnerabilities
PS01	C	Insecure social robot software design and lack of sound security assessment before deployment
PS02	P/S	Inadequate social behavior approach in social robot design to attract bystanders during abuse
PS03	S	Inadequate socially acceptable normative approach behavioral design for a robot in public spaces
PS04	C	Insecure software design that cannot detect anomalous behavior in social robot logs
PS05	C	Lack of complete stakeholder involvement in social robot privacy design research discussion
PS06	C	Insecure software design for social robots to ensure data security
PS07	C	Insecure software design to promote hardware security of sensors
PS08	P	Inefficient safety design for social robot–human interaction in shared workspaces
PS09	C	Inadequate security policy implementation of access control and authentication for emotional data
PS10	C	Lack of dynamic, scalable, and decentralized security solutions for social robots
PS11	C/S	Inadequate technical insights into how social robots can exploit human overtrust in social engineering
PS12	C	Inadequate face de-identification solutions for social robots
PS13	C	Inadequate hardware security design for the Linux kernel vulnerability that can easily be exploited through physical contact with a social robot (e.g., inserting a USB pen drive)
PSA01	C	Inadequate resources for secure social robot application design/development
PSA02	S	Inadequate design solutions for predicting and avoiding social robot abuse among children
PSA03	C	Insecure design and assessment of programmable robotic software platforms
PSA04	C	Inadequate software security design against malicious pdf files accessed by social robots
PSA05	S	Insufficient insights into how social robots can exploit human overtrust during social engineering
PSA06	C	Inadequate software security design to mitigate data privacy leaks of social robot sensors
PSA07	S	Insufficient anti-bullying program design using social robots
PSB01	P	Insufficient knowledge of the process of children abusing social robots in public spaces

* C =Cybersecurity, S = Social, P = Physical.

4.4. Attack Surface of Social Robots in Public Spaces

This section reports attacks on social robots in public places, the attack scenarios, impacts, and mitigation strategies proposed in the primary studies. It aims to provide an overview of social robots' attack surface in public spaces.

4.4.1. What Are the Reported Attacks on Social Robots in Public Spaces?

Attacks identified in this review are grouped into four categories. Cybersecurity attacks received the greatest attention at 67% (fourteen, PS01, PS04, PS05, PS06, PS07, PS10, PS11, PS12, PS13, PSA01, PSA03, PSA04, and PSA06), while 62% (thirteen, PS01, PS02, PS05, PS08, PS11, PS13, PSA01, PSA02, PSA03, PSA05, PSA06, and PSA07) reported physical attacks, compared to 24% (five, PS03, PS05, PS07, PS11, and PSA06) and 9.5% (two, PS05 and PSA01) for social and public space attacks. Out of the primary studies, 48% (10) reported more than one category of attack.

Of all the identified cybersecurity attacks (fourteen), software attacks accounted for 93% (thirteen), communication attacks 50% (seven), hardware attacks 43% (six), cloud

services attacks (three), social engineering 14% (two), and AI attacks 4% (one). A comprehensive list of all attacks identified in this review is shown in Table A8 of Appendix D.

Cybersecurity attacks. Using the CAPEC mechanism of attack classification [124], all cybersecurity attacks identified in primary studies were grouped into nine categories: (i) engaging in deceptive interactions, (ii) abusing existing functionality, (iii) manipulating data structures, (iv) manipulating system resources, (iv) injecting unexpected items, (v) employing probabilistic techniques, (vi) manipulating timing and state, (vii) collecting and analyzing information, and (viii) subverting an access control.

1. *Engaging in deceptive interactions*. It includes spoofing and manipulating human behaviors in social engineering. Variants of spoofing attacks include content, identity, resource location, and action spoofing. Not all these variants of spoofing attacks were identified in this review. Identity spoofing attacks include address resolution protocol (ARP) spoofing (PS01), signature spoofing (cold boot attack PS13), DNS spoofing (PSA04), and phishing (PS05, PS11, and PSA03). PS01 reported one account of an action spoofing attack (clickjacking attack). Seven studies (PS01, PS05, PS07, PS11, and PSA05) reported attacks related to manipulating human behavior, i.e., pretexting, influencing perception, target influence via framing, influence via incentives, and influence via psychological principles.
2. *Abusing existing functionalities*. It includes interface manipulation, flooding, excessive allocation, resource leakage exposure, functionality abuse, communication channel manipulation, sustained client engagement, protocol manipulation, and functionality bypass attacks. Interface manipulation attacks exploiting unused ports were reported in PS01. Flooding attacks resulting in distributed denial of service (DDoS) were also reported (PS10, PS13, and PSA03). Likewise, resource leakage exposure attacks resulting from CPU in-use memory leaks (PS13) and communication channel manipulation attacks in the form of man-in-the-middle attacks were reported (PS01, PS10, PS13, and PSA03).
3. *Manipulating data structures*. It includes manipulating buffer, shared resource, pointer, and input data. Buffer overflow and input data modification attacks were reported in PS13 and PS09, respectively.
4. *Manipulating system resources*. It includes attacks on software/hardware integrity, infrastructure, file, configuration, obstruction, modification during manufacture/distribution, malicious logic insertion, and contamination of resources. Some examples of attacks were identified in this category, i.e., physical hacking (PS05, PS09, PS10, and PS11), embedded (pdf) file manipulations (PSA04), obstruction attacks (jamming, blocking, physical destruction, PS02, PS10, PS13, PSA03).
5. *Injecting unexpected items*. It comprises injection and code execution attacks. Injection attack variants include parameter, resource, code, command, hardware fault, traffic, and object injection. Examples of reported attacks in the category include code injection attacks (PS01, PS04, PS13) and code execution attacks (PS01, PSA03, and PSA04).
6. *Employing probabilistic techniques*. It employs brute force and fuzzing. Brute force attacks on passwords and encryption keys were reported in PS01, PS13, and PSA01. Attacks resulting from unchanged the default administrators' username/password and dictionary brute force password attacks were also noted in PS01.
7. *Manipulating timing and state*. This class of attacks includes forced deadlock, leveraging race conditions, and manipulating the state. Forced deadlock attacks can result in denial of service (PS10, PS13, PSA03), while leveraging race conditions can result in a time-of-use attack (PS13). Manipulating states can result in various types of malicious code execution attacks (PS01, PSA03, PSA04).
8. *Collecting and analyzing information*. It includes excavation, interception, footprinting, fingerprinting, reverse engineering, protocol analysis, and information elicitation. Data excavation entails extracting data from both active and decommissioned devices and users. Interception involves sniffing and eavesdropping attacks (PS10 and PS13).

Footprinting is directed to system resources/services, while fingerprinting can involve active and passive data collection above the system to detect its characteristics (PSA03). Reverse engineering uses white and black box approaches to analyze the system's hardware components. Protocol analysis is directed at cryptographic protocols to detect encryption keys. Information elicitation is a social engineering attack directed at privileged users to obtain sensitive information (PS05 and PS11). In this review, some studies reported collecting and analyzing information attacks as surveillance (PS05, PS07, and PSA06).

9. *Subverting access control*. It includes exploits of trusted identifiers (PSA03), authentication abuse, authentication bypass (PSA01, PS09, PS13, and PSA03), exploit of trust in client (PS06), privilege escalation (PS01, PS09, and PS13), bypassing physical security (PS01), physical theft (PS05), and use of known domain credentials (PS01).

Physical attacks are safety-related attacks that harm humans or damage social robots. A social robot under cyber-attack can cause physical harm to humans; however, physical attacks in this context are most likely to result from system failures, malfunction, and inefficient system design. Physical attacks on humans in this context could be physical (PS01, PS08, PS13, PSA01, and PSA03) or psychological (PS01 and PS02). Physical attacks on social robots identified include violence against social robots (physical abuse, PS02), vandalism (PSA07), theft (PS05), bullying/maltreatment from children (PSA07), sabotaging a social robot's tasks (PSA07), verbal abuse (PS02), and obstructing a social robot's path (PSA02, PSA07, and PSB02).

Social attacks in this context refer to violations of social norms by social robots in public spaces due to inefficiencies in AI system design. If social robots cannot adhere to social norms during human interactions in public spaces, they may be viewed as social misfits. Examples of identified social norm violation attacks include: (i) personal space violation (PS03 and PS05), (ii) human trust exploitation (PS11 and PSA05), (iii) embarrassment to humans (PSA06), (iv) human deception and manipulation (PS11), and (v) exploiting users' preferences through targeted marketing (PS05).

Public space attacks in this study refer to damages to the environment resulting from social robot interaction or negative influences of natural environmental factors (e.g., fire, flood, rain, weather, wars) on the successful operation of the social robot in public spaces. In this review, PSA03 reported incorporating fire, safety, water, and local news into the robotic platform to prevent attacks related to natural environmental factors, while three studies reported instances of property damages resulting from attacks caused by social robots during interactions (PS05, PS13, and PSA01).

4.4.2. What Are the Reported Attack Scenarios for Social Robots in Public Spaces?

An attack scenario describes the steps and ways a threat actor will employ to exploit a vulnerability in a particular attack successfully [125]. The attack scenarios reported in the primary studies did not mention all the necessary steps. The template proposed by ENISA [126] was used to present four different hypothetical attack scenarios, drawing insights from primary studies in this SLR.

Table 8 shows "Attack Scenario 1" about social robot abuse by users, adapted from four primary studies (PS05, PSA02, PSA07, and PSB01).

Table 8. Attack Scenario 1—Social robot abuse by users (PS05, PSA02, PSA07, and PSB01).

SOCIAL ROBOT ABUSE BY USERS
DESCRIPTION
Threat actors may physically abuse a robot during interaction in public spaces due to a lack of constant supervision in such locations. Examples of such reported social robot abuse include (i) blocking the path of a social robot, (ii) hitting the social robots, (iii) blocking the sensors (e.g., LIDAR, cameras) with spray paint or masking tape, (iv) verbally abusing the social robot, (v) placing fake spoofing images/signs on the path of the social robot, (vi) vandalizing social robot components in a secluded location or stealing the whole unit. Maltreatment of this nature could affect the smooth operation of the social robot, thereby leading to physical damage and hindering service availability.

Table 8. *Cont.*

SOCIAL ROBOT ABUSE BY USERS	
IMPACT	
Medium—High: Depending on the attack, the impact could be medium to high. It may have a medium effect in the case of verbal abuse and physical obstruction of the social robot's path, in which case the social robot could try an alternate route. However, it is high in cases of physical damage to the robot or blocking critical sensors during social interaction.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Easy—Medium—Hard: Depending on the specific type of attack and the public space setting of the social robot.	**Medium—High**: In minor abuse cases, the cascade effect risk may be medium; however, in severe abuse scenarios, there may be high risks.
ASSET AFFECTED	**STAKEHOLDERS INVOLVED**
Hardware: Sensors, actuators, AI: AI model Software: Recognition and motion planning algorithms	Social robot hardware designers, software developers, and AI model developers. Social robot backend and frontend users.
ATTACK STEPS	
1. Reconnaissance: Threat actors gather information about the navigation path of the social robot and plan how to obstruct the social robot's path using suitable means (physical obstacles or spoofing images/road signs). **2. Weaponization and delivery**: Threat actors plant obstacles in the path of the social robot, causing the social robot to redirect their way to isolated locations where masked threat actors could spray paints on sensors or use adhesive masking tape to cover sensors (camera). Malicious actors could also attach explosives or tracking devices to social robots in such blind spot locations, which could be used in other areas. **3. Action on Objectives**: Threat actors could vandalize or steal the social robot at such a blind spot, use the attached tracking devices to monitor the social robot or its users, or trigger the explosive in specific desired locations. The objective may be to sabotage the smooth interaction of the social robot or disrupt service availability to users.	
RECOVERY TIME/EFFORT	**GAPS AND CHALLENGES**
Medium—High: In minor abuse scenarios, the recovering time may be medium, but in severe abuse cases, it may require a high recovery time.	(i) Authentication of unusual route changes, (ii) Detection of spoofing images/road signs, (iii) Design of efficient and robust AI model for social robots.
COUNTERMEASURES	
(i) Incorporating redundancy in hardware sensor design, (ii) Incorporating adversarial examples in hardening AI model design, (iii) Incorporating route validation during social robot navigation.	

Table 9 shows "Attack Scenario 2" about social robot compromise resulting from malicious file attachment access leading to malicious code execution adapted from two primary studies (PS01 and PSA04).

Table 9. Attack Scenario 2—Social robot compromise through malicious file attachment (PS01 and PSA04).

SOCIAL ROBOT COMPROMISE	
DESCRIPTION	
Threat actors may replace a genuine file (pdf or jpeg) with malicious versions. During social robot interaction, users may require information that is stored as pdf or jpeg files. Examples of such reported social robot compromise include (i) executing malicious code during pdf file access (PSA04) and (ii) executing malicious code during jpeg file access (PS01). Malicious code execution can result in software and application integrity attack in a social robot	
IMPACT	
High: Delivering a malicious file to a system is a key step towards the exploitation of other vulnerabilities. This attack's impact is high when no safeguards are in place.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Easy—Medium: There are several file scanning solutions that can easily detect such malicious files.	**Medium—High**: If the malicious code is executed without detection, the cascade effect risk will vary from medium to high.
ASSET AFFECTED	**STAKEHOLDERS INVOLVED**
Software: Operating system and applications	Software developers
ATTACK STEPS	
1. Reconnaissance: Threat actors gather information about the frequently accessed files for a given social robot case. **2. Weaponization and delivery**: Threat actors replace the genuine file with a malicious file having a fake file extension (.jpeg or .pdf) **3. Action on Objectives**: Once a social robot accesses a malicious file and malicious code execution is successful, threat actors could install additional malicious codes (malware) that would aid their command and control of such a system and execute their objectives.	

Table 9. *Cont.*

SOCIAL ROBOT COMPROMISE	
RECOVERY TIME/EFFORT	**GAPS AND CHALLENGES**
Medium—High: Depending on the stage and type of malicious code executed, the recovering time/effort may vary from medium to high.	(i) Authentication of files accessed by the social robot, (ii) Automatic anomaly detection of malicious content, (iii) Input validation for social robot interaction with users.
COUNTERMEASURES	
(i) Incorporating third-party antivirus and antimalware solutions, (ii) Incorporating MIME-sniffing protection in social robot software, (iii) Incorporating secure input validation for social robot applications interacting with users.	

Table 10 shows "Attack Scenario 3" about social robot insiders. It was adapted from three primary studies (PS01, PS13, and PSA04). It presents insights into how a threat actor could exploit exposed communication ports as an external actor or an insider threat to compromise the social robot software and hardware integrity (using a USB drive).

Table 10. Attack Scenario 3—Social robot compromise through exposed communication ports (PS01, PS13, PSA04).

SOCIAL ROBOTS AS INSIDER THREAT	
DESCRIPTION	
Threat actors may exploit exposed communication ports of a social robot while operating in public spaces using a USB pen drive. A malicious insider with authorized access may also want to compromise the system using the same means. Examples of such reported compromise by social robot insiders include (i) compromising software and hardware integrity using a malicious USB drive as an insider (PS01, PS13, and PSA03) and (ii) compromising social robot system integrity as an external user within proximity, using the same means.	
IMPACT	
High: A complete hardware and software integrity compromise due to this type of attack would greatly impact the social robot's operation.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium-Hard: Depending on the safeguards and protection in place.	**High**: For a successful social robot software and hardware compromise, the cascade effect risk would be high.
ASSET AFFECTED	**STAKEHOLDERS INVOLVED**
Hardware: Exposed communication ports. **Software**: Operating system and applications.	Hardware designer/manufacturer, software developers, and testing team
ATTACK STEPS	
1. Reconnaissance: Threat actors gather information about physically exposed communication ports of the social robot during interaction or usage. Malicious actors could also perform slow and difficult-to-detect vulnerability scans to detect active unused resources, applications, or communication ports. **2. Weaponization and delivery**: Threat actors could use other means to redirect the route of a social robot to an isolated location and insert a compromised USB drive to attack the software integrity of the social robot. **3. Action on Objectives**: Once a threat actor succeeds in delivering a payload through a USB drive, they can easily perform other objectives, like installing malware, escalating privileges, etc.	
RECOVERY TIME/EFFORT	**GAPS AND CHALLENGES**
Medium–High: The recovery effort may be medium to high, depending on the level of system compromise.	(i) Detection and mitigation against privileged and skilled insider threats, (ii) Hardware-assisted trust execution environment-based protection.
COUNTERMEASURES	
(i) Disabling unused ports before social robot deployment, (ii) Adopting the least privilege security principles for users, (iii) Ensuring the safe design of social robots without exposing their communication ports.	

Table 11 shows "Attack Scenario 4" about how threat actors could hack a social robot and use it for social engineering attacks. It was developed based on insights from six related primary studies (PS01, PS05, PS07, PS11, and PSA05). Moreover, other attack-related factors were considered, namely impact, ease of detection, cascade effect risk, assets affected, stakeholders involved, attack steps, recovery time/effort, gaps and challenges, and countermeasures. These additional attack-related factors emerged from the evaluation of these attack scenarios in which social robots could be exploited for social engineering attacks on humans.

Table 11. Attack Scenario 4—Social robot exploited as a social engineer (PS01, PS05, PS07, PS11, and PSA05).

SOCIAL ROBOTS EXPLOITED AS A SOCIAL ENGINEER	
DESCRIPTION	
Threat actors may exploit other social robot vulnerabilities and use them for social engineering and espionage attacks. Examples of such reported social engineering attacks include (i) extracting sensitive information from users during interaction (PS01, PS07, and PSA05), (ii) manipulating users' preferences during purchase (PS05, PSA05), (iii) exploiting the trust of users (PS11, PSA05), and (iv) spying on users (PS01, PS07). A hacked social robot could become a tool for corporate espionage and social engineering attacks.	
IMPACT	
High: The impact of a hacked robot as a tool for espionage and social engineering attacks could be very high, depending on the threat actor's objectives.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Medium-Hard: It may be challenging to detect an intelligent attempt by social robots to extract sensitive information from users, especially in low-awareness settings.	**High**: In the two scenarios above, the cascade effect risk is high
ASSET AFFECTED	**STAKEHOLDERS INVOLVED**
Hardware: Sensors and actuators. Software: Operating system and applications.	Hardware designer/manufacturer, software developers and testing team
ATTACK STEPS	
1. Reconnaissance: Threat actors gather information about the social robot, its operating environment, and its potential users. Malicious actors then search for specific known vulnerabilities of the social robots and plan their attack strategy. **2. Weaponization and delivery**: Threat actors could exploit any known vulnerability, install malware, escalate privilege, and gain command and control access to the social robot. **3. Action on Objectives**: Once a threat actor succeeds in the above steps, s/he could use the cameras of the social robot to spy on users, control the social robot to extract information from the users using known algorithms (PS11), exploit users' trust, and influence users' purchase preferences during interactions.	
RECOVERY TIME/EFFORT	**GAPS AND CHALLENGES**
Medium–High: The recovery effort may be medium to high, depending on the level of system compromise.	(i) Detection and mitigation against social engineering attacks for social robots in public spaces.
COUNTERMEASURES	
(i) Creating user awareness, (ii) Ensuring robust and secure social robot design, (iii) Ensuring the least privileged security design.	

4.4.3. What Are the Reported Attack Impacts of Social Robots in Public Spaces?

The impact of attacks on social robots in public spaces is presented from three perspectives: (i) cybersecurity objectives, (ii) users, and (ii) organizations.

Impacts on cybersecurity objectives. There are three cybersecurity objectives proposed by NIST [127]—confidentiality, integrity, and availability—to group attack impact based on information security objectives. The opposites of these three security objectives in information system security are disclosure, alteration, and destruction/denial (DAD). Loss of integrity (alteration) was reported in four studies (PS01, PS13, PSA02, and PSA03) as the impact of attacks on the information system. Disclosure (loss of confidentiality) was reported in five studies (PS01, PS06, PS13. PSA03, and PSA05). Moreover, six studies (PS01, PS02, PS06, PS13, PSA02, and PSA03) reported the loss of availability (destruction/denial of service), and a violation of one or more security objectives above was reported as a privacy violation and reported by four studies (PS06, PS07, PS12, and PS13).

Impacts on users and organizations. The impact of an attack on users and organizations could have different dimensions, such as physical, economic, psychological, reputational, and societal [128]. The physical impact could include (i) loss of life (PSA03), (ii) harm to users or employees (PS01, PS04, PS08, PS10, PSA02, and PSA03), (iii) damage to properties and other assets (PS01, PS04, PSA02, PS08, PSA01, PS02, and PSA03), (iv) physical loss of assets due to theft, (v) reduced performance or complete downtime of an asset (PS01, PS02, PSA02, and PSA03), and (vi) a hacked social robot could be a vulnerability source to other organizational assets (PS01). Economic impact includes financial loss resulting from (i) income loss due to downtime, disrupted services, and unsatisfied customers' experience, (ii) repair, investigation, and public relations cost, (iii) ransom cost and increase in insurance in premium due to an increase in perceived risk, (iv) loss in customers' loyalty, goodwill, and brand depreciation, and (v) cost of regulatory sanctions/fines, claims

for injuries and deaths, and so on (reported in PS10 and PSA01). Psychological impacts on employees and customers of a museum were reported in PSA01, which could be in the form of embarrassment, low satisfaction, or discomfort. Reputational damage was reported in PS04 and PSA03. The societal impact of attacks on social robots in public spaces was not identified in the primary studies; however, it is worth noting that any attack on humans and organizations impacts our society.

4.4.4. What Are the Reported Attack Mitigations on Social Robots in Public Spaces?

Attack mitigation depends on the type of attack and the sub-component receiving such an attack. About 14.3% (three studies, PS05, PS11, and PSA05) of the twenty-one primary studies identified potential vulnerabilities in social robots, but they did not mention a mitigation strategy against such attacks. PS05 discussed privacy concerns on social robots using focus groups, but mitigations to these privacy concerns were not discussed. PS11 and PSA05 reported how social robots could exploit humans in social engineering attacks without proposing mitigations to such attacks (see more details of proposed attack mitigations reported in Table A9 of Appendix D).

5. Discussion

This section discusses the implications of the findings based on previous literature, the threats to the validity of our study, our proposed taxonomy for threat actors and landscape in this domain, and our recommendations.

5.1. Implications of Our Findings

The threat landscape of social robots in public spaces is a transdisciplinary research area involving social science (public space management), cognitive sciences, psychology, Human–Computer Interaction (HCI), AI, computer science, robotics, and engineering with rapidly growing interest [76]. This research field is not an extension of just one discipline; it should draw insights from outside HRI to ensure successful implementation and acceptance [129].

5.1.1. Research Trends of Social Robots in Public Spaces

This SLR shows that only 1.4% (21 out of 1469 papers) of the search results satisfied the selection criteria for empirical research in social robots in public spaces, indicating very little empirical research. Pepper and Nao, well-known commercial social robots, were used in 23.8% (five) of studies, indicating a low adoption of actual social robots for academic research. About 76% (16 studies) manually customized vision, navigation, AI, and cloud services for the social robot used in their studies. Although the authors did not state the reason for the low adoption of well-known commercial social robots in our reviewed studies, one plausible explanation is the high cost of Pepper (about USD 20,000 for universities/organizations in 2021 [130]) and lack of technical expertise in integrating AI and cloud services. Our study shows a growing interest in the field, as reported by other existing literature [131,132]. However, there is a need for more funding and empirical research on social robots in public spaces.

5.1.2. Threat Actors of Social Robots in Public Spaces

A technical description of the threat actors related to robots in public spaces will inform security components design, enable interoperability, and eliminate ambiguity resulting in a machine-understandable threat actor attribution/characterization that will ensure automatic machine inference. The threat actors, motives for attacks, and attack outcomes identified in our SLR are consistent with existing reports on cybersecurity threats [46,57,93,109,133]. Our study also confirmed that a hacked social robot could be a threat actor to humans. However, we observed that our primary studies did not report some potential threat actors associated with supply chain, cloud services, and AI services. A specific threat landscape in this context should cover all possible sources of threat actors;

hence, a taxonomy of threat actors can benefit researchers and practitioners interested in developing security mechanisms adapted to each type of threat in this context.

5.1.3. Identifying Assets, Threats, and Vulnerabilities of Social Robots in Public Spaces

In this SLR, we identified two threat directions, seven asset categories, four threat groups, and 21 specific vulnerabilities addressed by our primary studies for social robots in public spaces. The threat direction, as reported, incorporates social robots' safety and security, which is consistent with previous studies, e.g., Mayoral-Vilches [79] and Alzoka-Kirschegen [49]. Our asset classification is in line with Mitre's CAPEC attack domain categorization [70] and the sub-component groups reported by Yaacoub et al. [71]; however, our review complements those studies by including supply chain and AI as assets of a robotics system, since the role of AI and the supply chain is indispensable for a successful operation. The vulnerabilities discussed in this study are peculiar to the works of our primary studies, as there are other known vulnerabilities that may not be reported in this situation.

5.1.4. Attack Surface of Social Robots in Public Spaces

Traditionally, the attack surface is an enumeration of entry points to a system, component, or environment. This study identified the assets and stakeholders of social robots in public spaces and explored the attack surface based on attacks identified in the primary studies and the mechanism of attacks proposed by Mitre [124]. Beyond cyber-attacks, other categories of attacks were identified, e.g., physical, social, and public space attacks. A complete risk assessment, of which threat landscape is an input, should anticipate all possible threats and attacks. The four attack scenarios presented in this study aim to illustrate the exploitation of vulnerabilities in this context. These scenarios are based on our SRL and inspired by the ENISA report on the uptake of AI in autonomous driving [126].

5.2. Limitations and Threats to Validity

In this subsection, we present the limitations, threats to the validity of this study, and measures taken to minimize such threats. Specifically, we considered the following four threats to validity according to Claes et al. [134]: construct, internal, conclusion, and external validity.

5.2.1. Construct Validity

Construct validity measures how closely this study actually investigates social robots' threat landscape in public spaces. This threat emerges from a lack of empirical evidence in this area. To minimize this threat, a search string consisting of relevant keywords addressing the threat landscape of social robots in public spaces was formulated, tested, and validated in our research protocol. We ensured that the focus of this review was on social robots/humanoids and that studies addressing key aspects like threats, vulnerabilities, and attacks were included in this review. We acknowledge the limitation of restricting our search to five academic bibliographic databases; however, these databases were recommended by Kitchenham and Charters [97] and adopted in previous reviews on this domain [98]. Additionally, we conducted a rigorous snowballing process to include additional relevant studies in this field.

5.2.2. Internal Validity

Internal validity measures how trustworthy a study's cause-and-effect relationships or conclusions are. It can occur in research due to systematic errors and authors' bias during data extraction. To minimize internal validity, we ensured that our protocol was based on well-established guidelines for performing SLRs [97]. Moreover, two researchers independently conducted the initial search. However, there was a discrepancy on SpringerLink (Researcher A obtained 252 while Researcher B obtained 495). We suspected this might be due to differences in the access rights of each researcher. The results of Researcher B

(495) were used for the review. We also observed slight variations in the search results when the URLs were validated in September 2022. The search result for IEEE increased by one, ACM increased by two, and ScienceDirect decreased by one. We developed a data extraction form to ensure consistency in our data extraction process. We also removed duplicate studies and evaluated the quality of all included studies.

5.2.3. External Validity

External validity measures the extent to which this study's results are generalizable. We acknowledge the limitation of restricting our primary studies' selection to academic databases; there is the possibility of missing research that is published in other databases, including grey literature such as white papers, technical reports, or work in progress, which were excluded from this study. Also noteworthy is the language restriction that excluded studies in other languages that could have relevant research on this topic. In our attempt to address the social robot's domain, we may have omitted other relevant studies that did not capture the keywords used to formulate the search string. Despite these limitations, this SLR contributes to extending the knowledge of the social robot's threat landscape in public spaces.

5.3. Recommendations and Future Works

The following are our recommendations from the findings of this SLR:

1. Academic researchers and industrial practitioners should carry out further empirical research to test and validate the threats proposed in this study. This will provide valuable insights into the security of human–social robot interactions in public spaces.
2. Stakeholders in social robots in public spaces should develop a security framework to guide social robot manufacturers, designers, developers, business organizations, and users on the best practices in this field. This transdisciplinary task will require input from all stakeholders.
3. Regulatory authorities should develop a regulatory standard and certification for social robot stakeholders. The existing ISO 13482:2014 on robots, robotic devices, and safety requirements for personal care robots do not fully address the needs of social robots in public spaces [37]. Such standards will enable users and non-experts to measure and ascertain the security level of social robots.
4. Social robot designers and developers should incorporate fail-safe, privacy-by-design, and security-by-design concepts in social robot component development. Such design could incorporate self-repair (or defective component isolation) capabilities for social robots in public spaces.
5. Entrepreneurs and start-ups should be encouraged by stakeholders in the areas of cloud computing and AI services. This will foster development and easy adoption of the technology.

In future work, we will develop a security framework for social robots in public spaces. Moreover, we will create a threat model for different use cases to test and validate such a security framework.

6. Taxonomy for Threat Actors and Threat Landscape for Social Robots in Public Spaces

By reviewing our primary studies and related works, we could not find any taxonomy for the threat actors or landscape for social robots in public spaces. As a contribution to this emerging domain, we propose a preliminary taxonomy for threat actors and landscapes for social robots in public space based on the findings of this study and its related works. A specific taxonomy will provide stakeholders (e.g., social robot designers, developers, policymakers, and researchers) with a shared vocabulary for communicating attacks, issues, improvements, and processes in this field.

6.1. Taxonomy for Threat Actors of Social Robots in Public Spaces

The taxonomy for threat actors for social robots in public spaces proposed in this study has four elements: internal, external, supply chain, and public space actors, as shown in Figure 5.

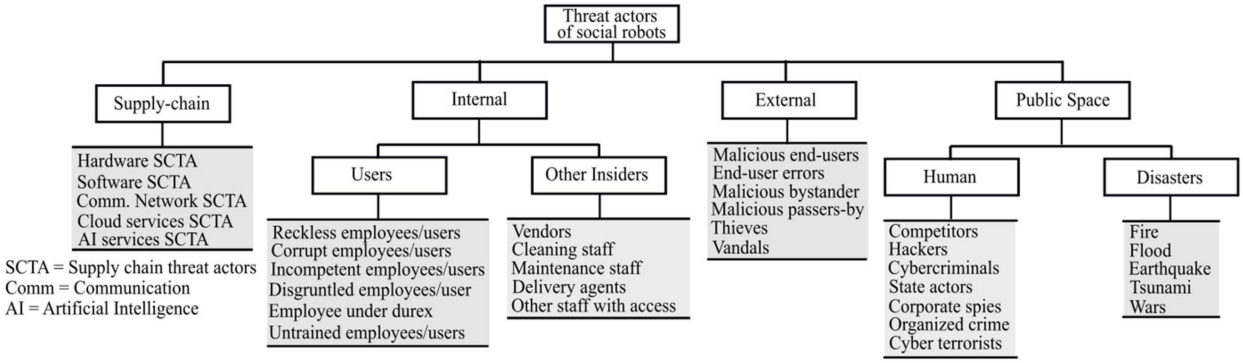


Figure 5. Overview of taxonomy for threat actors of social robots in public spaces.

1. **Internal threat actors** include employees, authorized users, and other organization staff with internal access. The insider threats posed by these actors could be intentional or non-intentional (mistakes, recklessness, or inadequate training). A particular example of an insider threat is authorized users under duress (e.g., a user whose loved ones are kidnapped and compelled to compromise). Other people with inside access who are potential threat actors could be vendors, cleaning staff, maintenance staff, delivery agents, sales agents, and staff from other departments, among others.
2. **External threat actors** are those outside the organization, often without authorized access to the social robot system or services. These actors could be physically present within public spaces or in remote locations. Examples of external threat actors include hackers, cyber criminals, state actors, competitors, organized crime, cyber terrorists, and corporate spies, among others.
3. **Supply chain threat actors** create, develop, design, test, validate, distribute, or maintain social robots. Actors that previously or currently had access to any sub-component of the social robot system, who can create a backdoor on hardware, software, storage, AI, and communication, fit into this group. A direct attack on any of these actors could have a strong implication for the security of social robots. This supply chain taxonomy is aligned with ENISA's threat landscape for supply chain attacks [135].
4. **Public space threat actors** could be humans (internal or external) or disasters (natural or man-made) [136] that are within the physical vicinity of the social robot. Physical proximity to the social robot is a key consideration for this group of actors. Disaster threat actors in the public space could be fire, flood, earthquake, tsunami, volcanic eruptions, tornadoes, and wars, among others. In contrast, human threat actors in a public space context could be malicious humans (e.g., users, end users, bystanders, passers-by, thieves, vandals, and saboteurs) within a public space of the social robot. It is possible for a threat actor to belong to more than one group in this taxonomy.

Our proposed threat actor's taxonomy agrees with previous studies in cybersecurity and contributes specifically to social robots in the public space use context. Table 12 shows a comparison of our taxonomy with related taxonomies. The focus of those taxonomies is external threat actors and malicious/incompetent insiders.

Table 12. Comparison of our proposed taxonomy with related works.

Threat Actor Group	Threat Actors in	[48]	[71]	[137]	[59]	[88]	This SLR
Supply Chain	Malicious/Incompetent hardware stakeholders		✓				✓
	Malicious/Incompetent software stakeholders		✓				✓
	Malicious/Incompetent cloud service providers						✓
	Malicious/Incompetent communication service providers						✓
	Malicious/Incompetent AI model stakeholders						✓
External	Competitor	✓	✓	✓		✓	✓
	Hackers/Cyber criminals	✓	✓	✓		✓	✓
	Cyber terrorists	✓	✓	✓	✓	✓	✓
	State-sponsored actors	✓	✓	✓	✓	✓	✓
	Corporate espionage group		✓	✓		✓	✓
	Organized criminal groups (hacktivists and hackers for hire)	✓	✓	✓	✓	✓	✓
Internal	Malicious/Incompetent insider (corrupt or reckless or untrained employee/user)	✓	✓	✓		✓	✓
	Employees under duress from external attackers						✓
	Disgruntled employee			✓	✓	✓	✓
Public space	Natural factors (fire, flood, thunder, earthquake, etc.)						✓
	Wars						✓
	Pandemics						✓
	Malicious end users/bystanders/passers-by						✓

6.2. Taxonomy for Threat Landscape of Social Robots in Public Spaces

We proposed a threat landscape for social robots in public spaces based on insights from this SLR and previous related works. Figure 6 depicts our proposed threat landscape, which is grouped into four categories: physical, cybersecurity, social, and public space threats.

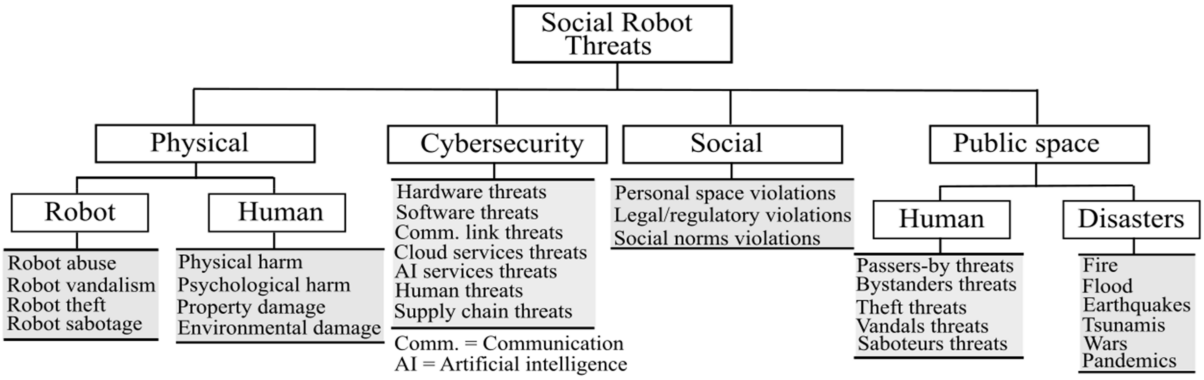


Figure 6. Overview of taxonomy for the threat landscape of social robots in public spaces.

1. **Physical threats** are safety-related threats to social robots and humans. Social robot abuse, vandalism, sabotage, and theft are some physical threats directed at social robots in public spaces. Social robots operating in public spaces pose the threat of physical/psychological harm and property (assets) and environmental damage to humans.
2. **Social threat**. Potential threats to personal space and legal/regulatory and social norm violations fall under the social threat landscape.

3. **Public space threats**. Strict regulations on sensitive data collection exist in the public space domain. As with the case of threat actors, we considered disaster and human threats affecting public space.
4. **Cybersecurity threats** can originate from different sources. Therefore, a taxonomy based on Mitre's CAPEC domain of attacks [70] is proposed. Moreover, it complements the proposal of Yaacoub et al. [71] on robotics cybersecurity, as it incorporates specific aspects of threats to social robots in public spaces.

Figure 7 illustrates our proposed cybersecurity threat taxonomy. It has seven components: hardware, software, communication, cloud services, AI services, human (social engineering), and supply chain threats.

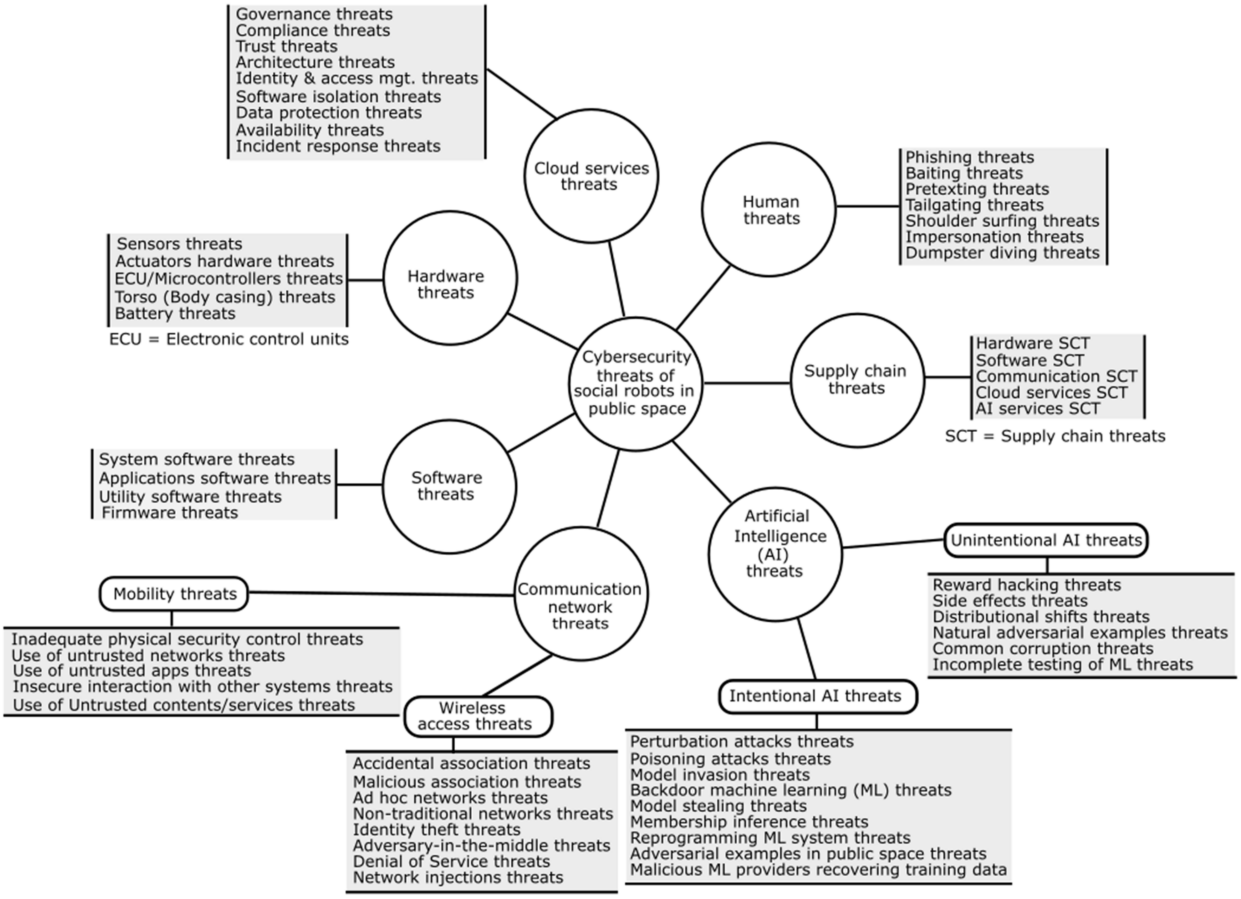


Figure 7. Overview of the cybersecurity threat landscape of social robots in public spaces.

1. **Hardware threats** are threats to sensors, actuators, electronic control units (ECUs), social robot bodies (casing), and batteries. Li et al. presented a survey of hardware trojan threats in [138], while Sidhu et al. [139] presented similar threats from an IoT perspective.
2. **Software threats** are threats to operating systems, applications (including third-party apps), utilities, and firmware (embedded software). Tuma et al. presented a systematic review of software system threats in [140].
3. **Supply chain threats**, like threat actors, could arise from any of the following: supply chains, hardware, software, communication, cloud services, and AI services. A comprehensive analysis of supply chain threats is presented by ENISA in [135].
4. **Human threats**, also known as social engineering, include phishing, baiting, pretexting, shoulder surfing, impersonation, dumpster diving, and so on. A comprehensive systemization of knowledge on human threats is presented by Das et al. in [141].

5. **Communication network threats** address two specific features of the communication systems of social robots in public spaces: wireless and mobility. According to [142,143], the wireless communication networks expose them to (i) accidental association, (ii) malicious association, (iii) ad hoc networks, (iv) non-traditional networks, (v) identity theft, (vi) adversary-in-the-middle, (vii) denial of service, and (viii) network injection threats. According to [143], the mobile nature of social robots' interactions in public space imposes the following threats: (i) inadequate physical security control, (ii) use of untrusted networks/apps/contents/services, and (iii) insecure interaction with other systems.
6. **Cloud services**, according to NIST SP 800-144 [144], introduce the following nine threats: (i) governance, (ii) compliance, (iii) trust, (iv) architecture, (v) identity and access management, (vi) software isolation, (vii) data protection, (viii) availability, and (ix) incident response threats.
7. **AI service threats**, according to the AI threat landscape of Microsoft Corporation [60], lead to intentional and unintentional failures. Intentional AI failure threats include (i) perturbation attacks, (ii) poisoning attacks, (iii) model invasion, (iv) backdoor models, (v) model stealing, (vi) membership inference, (vii) reprogramming of the model, (viii) adversarial examples in public spaces, and (ix) malicious model providers recovering training data. Unintentional threats include (i) reward hacking, (ii) side effects, (iii) distributional shifts, (iv) natural adversarial examples, (v) common corruption, and (vi) incomplete testing of ML.

7. Conclusions

This study systematically reviews and analyses empirical studies on the threat landscape of social robots in public spaces. Specifically, this review aims to report (i) the trend of empirical research in this field, (ii) the threat actors and their motives for attacks, (iii) the assets, threats, and vulnerabilities of social robots in public spaces, and (iv) the attack surface for this emerging domain. The initial search returned 1469 studies, and then 21 empirical studies that satisfied the selection criteria were included in this review. Our results reveal two threat directions, four threat categories, three research methods, ten application domains, thirty-three threat actors, seven attack motives, eight attack outcomes, seven asset groups, seven varieties of attacks, and four attack scenarios. Apart from well-known cybersecurity threats, this review identified insights into physical, social, and public space threats.

The findings of this study are significant to stakeholders interested in addressing the security and privacy concerns of social robots in public spaces. Based on the findings, a preliminary taxonomy for threat actors and the threat landscape of social robots in public spaces was proposed. The threat actor taxonomy will enhance the development of computer-understanding solutions for threat actors in social robotics. Moreover, the proposed threat landscape will enrich the risk assessment, measurement, and management of social robots in public spaces. The insights from other emerging sub-components of the social robotics system, such as AI and cloud services, will provoke further research in these directions. Future work will develop a threat model and security framework for a social robot used in a water ferry to provide information to users.

Supplementary Materials: The following supporting information can be downloaded at: https://data.mendeley.com/datasets/c28vkncvw2/draft?a=38164945-edff-4794-ae66-b89ddcf7360b (accessed on 5 December 2022). Replication package: Information source and search url.docx, Repository.xlsx, data extraction checklist.docx, and quality assessment questions.docx.

Author Contributions: Conceptualization, S.O.O., M.S.-G. and R.C.-P.; methodology, S.O.O. and M.S.-G.; investigation, S.O.O. and J.K.H.; data curation, S.O.O. and J.K.H.; writing—original draft preparation, S.O.O.; writing—review and editing, M.S.-G., V.G. and R.C.-P.; supervision, R.C.-P.; project administration, R.C.-P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Norwegian Research Council under the SecuRoPS project "User-centered Security Framework for Social Robots in Public Spaces" with project code 321324.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. List of typical sensors used in social robots.

Sensor Type	Sensor	Description with Robot Application Examples
Internal	Potentiometer	An internal position sensor, e.g., a rotary potentiometer, is used for shaft rotation measurement. Masahiko et al. used a rotary potentiometer to measure the musculoskeletal stiffness of a humanoid robot [145].
	Optical encoder	A shaft connected to a circular disc containing one or more tracks of alternating transparent and opaque areas is used to measure rotational motion. Lang et al. employed an optical encoder and other sensors for object pose estimation and localization in their mobile robot [146].
	Tachometer	It provides velocity feedback by measuring the motor rotating speed within the robot. Wang et al. employed a tachometer in a camera wheel robot design [147].
	Inertia Measurement Unit (IMU)	A module containing three accelerometers, three gyroscopes, and three magnetometers responsible for robot gait/stability control [148]. Ding et al. employed an intelligent IMU for the gait event detection of a robot [149].
	Accelerometer	It measures the change in speed of a robot. It can also be used in gait selection. Kunal et al. used this sensor in the implementation of a 5 DoF robotic arm [150].
	Gyroscope	An angular motion detector or indicator. They measure the rate of rotation. Kim et al. employed a gyroscope to design and control a sphere robot [151].
Range	Ultrasonic sensor	A sound wave measures the distance between the sensor and an object. They are used for navigation and obstacle avoidance [152]. Liu et al. employed this sensor in their mobile robot localization and navigation design [153].
	RGB Depth Cameras	It consists of an RGB camera, a depth sensor and a multiarray microphone that produces both RGB and depth video streams [40]. It is used in face recognition, face modeling, gesture recognition, activity recognition, and navigation. Bagate et al. employed this sensor in human activity recognition [154].
	Time-of-flight (ToF) cameras and other range sensors	ToF sensors use a single light pulse to measure the time it takes to travel from the sensor to the object. Other range-sensing approaches include stereo cameras, interferometry, ToF in the frequency domain, and hyper-depth cameras [40].
	LiDAR	Light Imaging Detection and Ranging employs a laser scanning approach to generate a high-quality 3D image of the environment. Its application is limited by reflection from glass surfaces or water. Sushrutha et al. employed LiDAR for low-drift state estimation of humanoid robots [155].
	RADAR	Radio detection and ranging use radio waves to determine the distance and angle of an object relative to a source. Modern CMOS mmWave radar sensors have mmWave detection capabilities. Guo et al. developed an auditory sensor for social robots using radar [156].
Touch	Tactile sensor	Tactile sensors are used for grasping, object manipulation, and detection. It involves the measurement of pressure, temperature, texture, and acceleration. Human safety among robots will require the complete coverage of robots with a tactile sensor. Different types of tactile sensor designs include piezoresistive, capacitive, piezoelectric, optical, and magnetic sensors [157]. Avelino et al. employed tactile sensors in the natural handshake design of social robots [158]. Sun et al. developed a humanlike skin for robots [159]. This also covers research on robot pains and reflexes [160].
Audio	Microphone	An audio sensor for detecting sounds. Virtually all humanoid robots have an inbuilt microphone or microphone array [161].
Smell	Electronic nose	A device for gas and chemical detection similar to the human nose [162]. Eamsa-ard et al. developed an electronic nose for smell detection and tracking in humanoids [163].
Taste	Electronic tongue	A device with a lipid/polymer membrane that can evaluate taste objectively. Yoshimatsu et al. developed a taste sensor that can detect non-charged bitter substances [164].

Table A1. *Cont.*

Sensor Type	Sensor	Description with Robot Application Examples
Vision	Visible Spectrum camera	Visible light spectrum cameras are used for the day vision of the robot. They are passive sensors that do not generate their own energy. Guan et al. employed this type of camera for mobile robot localization tasks [165].
	Infrared camera	Infrared cameras are suitable for night vision (absence of light) using thermal imaging. Milella et al. employed an infrared camera for robotic ground mapping and estimation beyond visible light [41].
	VCSEL	Vertical-cavity surface-emitting laser (VCSEL) is a special laser with emission perpendicular to its top surface instead of its edge. It is used in 3D facial recognition and imaging due to its lower cost, scalability, and stability [166]. Bajpai et al. employed VCSEL in their console design for humanoids capable of real-time dynamics measurements at different speeds [167].
Position	GPS	A Global Positioning System is used for robot navigation and localization. Zhang et al. employed GPS in the path-planning design of firefighting robots [168].
	Magnetic sensors	Magnetic sensors are used for monitoring the robot's motor movement and position. Qin et al. employed a magnetic sensor array to design real-time robot gesture interaction [169].

Appendix B

Table A2. Summary of snowballing.

PS	Ref	Citations	Backwards	Forward	Included	ID
			ROUND 1			
PS01	27	34	0	1	1	PSA01
PS02	36	50	1	0	1	PSA02
PS03	53	3	0	0	0	
PS04	9	5	0	0	0	
PS05	36	12	0	0	0	
PS06	31	3	0	0	0	
PS07	32	31	0	0	0	
PS08	21	14	0	0	0	
PS09	29	57	0	2	2	PSA03–PSA04
PS10	13	5	0	0	0	
PS11	39	5	1	0	1	PSA05
PS12	71	61	1	0	1	PSA06
PS13	46	2	0	0	0	
			ROUND 2			
PSA01	23	4	0	0	0	
PSA02	25	169	0	1	1	PSB01
PSA03	36	1	0	0	0	
PSA04	16	16	0	0	0	
PSA05	44	0	0	0	0	
PSA06	55	57	0	0	0	
PSA07	41	34	0	0	0	
			ROUND 3			
PSB01	18	59	0	0	0	

Appendix C

Table A3. Quality assessment score of our primary studies.

#	ID	QAS1	QAS2	QAS3	QAS4	QAS5	QAS6	QAS7	QAS8	QAS9	QAS10	QAS11	QAS12	QAS13	QAS14	QAS15	Total (%)
1	PS01	1	1	1	1	1	1	1	1	1	1	1	0.5	1	0	1	90
2	PS02	1	1	1	0.5	1	1	1	1	1	1	0.5	0.5	1	0	1	83.3
3	PS03	1	0.5	1	0.5	1	1	1	1	1	1	0.5	0.5	1	0	1	80
4	PS04	1	1	1	0.5	1	1	1	1	1	1	1	0.5	1	0	1	86.7
5	PS05	1	0.5	1	0.5	1	1	1	1	1	1	0.5	0.5	0.5	0	1	76.7
6	PS06	1	1	1	0.5	1	1	0.5	1	0.5	0.5	1	0.5	0.5	0	1	73.3
7	PS07	1	0.5	0.5	0.5	0.5	1	1	1	0.5	1	0.5	0.5	1	0	1	70
8	PS08	1	0.5	1	0.5	0.5	1	1	1	0.5	1	0.5	0.5	1	0	1	73.3
9	PS09	1	1	1	0.5	1	0.5	1	1	1	1	0.5	0.5	0.5	0	1	767
10	PS10	1	1	1	0.5	1	1	0.5	1	1	1	0.5	0.5	0.5	0	1	76.7
11	PS11	1	0.5	1	0.5	1	1	1	0.5	1	1	0.5	0.5	0.5	0	1	73.3
12	PS12	1	1	1	1	0.5	1	1	1	1	1	0.5	0.5	0.5	1	1	86.7
13	PS13	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	93.3
14	PSA01	1	1	1	0.5	1	1	1	1	1	1	1	0.5	0.5	0	1	83.3
15	PSA02	1	0.5	1	0.5	0.5	1	1	1	1	1	0.5	0.5	0.5	0	1	73.3
16	PSA03	1	1	0.5	0.5	1	1	0.5	1	1	1	1	0.5	0.5	0	1	76.7
17	PSA04	1	0.5	1	0.5	1	1	1	1	1	0.5	0.5	0.5	0.5	0	1	73.3
18	PSA05	1	0.5	0.5	0.5	0.5	1	1	1	1	1	0.5	0.5	0.5	0	1	70
19	PSA06	1	1	1	0.5	0.5	1	1	1	1	1	0.5	0.5	0.5	0	1	76.7
20	PSA07	1	1	1	0.5	1	1	1	1	1	1	0.5	0.5	0.5	0	1	80
21	PSB01	1	0.5	1	0.5	0.5	1	1	1	1	1	0.5	0.5	0.5	0	1	73.3

Table A4. Overview of Country affiliation.

#	ID	Year	Country of Research	Affiliation
1	PS08	2014	Brunei	Academia
2	PSA07	2021	Canada	Academia
3	PS12	2021	China	Academia
4	PSA04	2020	China	Mixed
5	PS09	2019	China, Saudi Arabia, Egypt	Academia
6	PSA06	2018	China, USA	Academia
7	PS03	2021	Denmark, Netherlands	Mixed
8	PSA01	2019	Germany, Luxembourg	Academia
9	PSA03	2019	India, Oceania	Academia
10	PS04	2019	Italy	Academia
11	PS11	2020	Italy	Mixed
12	PS13	2020	Italy	Academia
13	PSA05	2018	Italy	Academia
14	PSA02	2015	Japan	Mixed
15	PSB01	2020	Japan	Mixed
16	PS06	2020	Portugal	Academia
17	PS10	2019	Romania, Luxembourg, Denmark, France	Mixed
18	PS01	2018	Sweden, Denmark	Academia
19	PS02	2018	USA	Academia
20	PS05	2017	USA	Academia
21	PS07	2016	USA, China	Academia

Table A5. Overview of primary studies, research methods, and types.

Research Method	Research Types	IDs
Mixed	Experiment and use case	PS10
	Experiment and Observation	PSA02, PS11, PSB01
	Experiment, Questionnaire, and Observation	PSA05
	Observation (Crowdsourced study) and Survey	PSA07
Qualitative	Focus Group	PS05
	Observation (Between-subject study)	PS02
Quantitative	Experiment and Questionnaire	PS03
	Experiment and Online survey	PS07
	Experiment	PS01, PS04, PS06, PS08, PS09, PS12, PS13, PSA01, PSA03, PSA04, PSA06

Appendix D

Table A6. Summary of threat actors identified in this review.

Actors	Description	IDs
Academic research groups	A team of researchers, usually from the same faculty, who are experts in the same field and are collaborating on the problem or topic.	PSA01
Adversaries	A person, group, organization, or government that engages in a harmful activity or intends to do so.	PSA04
Centralized trusted entities	A third party to whom an entity has entrusted the faithful performance of specific services. An entity has the option to represent itself as a trustworthy party.	PS06
Children	A child who has not reached puberty or reached the legal age of maturity.	PS02, PSA02, PSA05
Competitors	An individual, group, or business that competes with others.	PSA03
Cyber criminals	An individual, group, or business that is involved in Internet-based criminal conduct or illegal activities.	PSA03
End users	A user who is trusted and has the authority to use the services of a social robot.	PS10
External attackers	Any external party acting to compromise a social robot or try to take advantage of a social robot's known vulnerabilities.	PS13, PSA01
Human actors	A person or group responsible for harmful, prohibited, or anti-social behavior.	PSA07
Illegal users	A person or group that is not allowed by law to use the services of a social robot.	PSA06
Insiders	A person or thing inside the security perimeter who has permission to use system resources but who misuses them against the wishes of the people who gave them to them.	PS01, PS13, PSA03
Invader	A person or group that uses force or craft to take control of another person's space or resources without the owner's consent.	PSA06
Malevolent user	A user who is creating harm or evil or wishing to do so.	PS13
Malicious attacker	A person, group, organization, or government that either intended to harm a social robot or to steal personal data from it.	PS01, PSA01, PSA03
Malicious user	A person, group, organization, or government with access rights that either intended to harm a social robot or to steal personal data from it.	PS09, PS13
Motivated attacker	An attacker with a specific motive.	PS01
Non-government gangs	A gang of criminals that collaborates.	PSA01
Others (Any attacker)	Any other type of attacker.	PS01
Privileged user	A user who has been granted permission (and is therefore trusted) to carry out security-related tasks that regular users are not permitted to do.	PS13
Remote operator	An operator interacting outside of a security perimeter with a social robot.	PSA04
Root user	A trusted user who has the authority to do security-related tasks that are not appropriate for regular users.	PS13
Skilled individual	Someone possessing the skills required to do a task or job effectively.	PSA01
Social engineers	Someone who uses others' confidence and trust to manipulate them into disclosing private information, granting unwanted access, or committing fraud.	PS11, PSA05
Social robots	An intelligent robot capable of human social interaction while observing social norms.	PS03, PS08
State level intelligence	A government group responsible for acquiring foreign or local information.	PSA01
Unauthorized party	A person or group that is not given logical or physical access to the social robot.	PS10
Disgruntled staff	A staffperson who is displeased, irritated, and disappointed regarding something.	PSA03
Spy	A person who covertly gathers and disseminates information about the social robot or its users.	PS07, PS13, PSA03
Wannabes	A person who is unsuccessfully attempting to become famous.	PS13

Table A7. Motives for cyber-attacks identified in this study.

Description of Cyber-Attack Motive	IDs
Information gathering (Reconnaissance)	
Using port scanning to detect Pepper's vulnerabilities	PS01
Conducting surveillance on users through a social robot	PS05
Retrieving users' identity information through a recovery attack	PS09
Gathering users' data through sniffing attacks on communication between robots and cloud	PS10
Using social robots for social engineering attacks to retrieve users' background data	PS11
Conducting cyber-espionage and surveillance on users through social robotic platforms	PS13
Social robots' sensors collect a lot of users' sensitive data during interaction, which an attacker tries to access during an attack	PSA05
Exploiting human overtrust in social robots during a social engineering attack on users	PSA05
Gaining/Escalating privileges	
Gaining and escalating privileges due to unsecured plain-text communication between social robots and cloud	PS01
Gaining access control privileges at the edge cloud due to inadequate security	PS09
Gaining privileges through a man-in-the-middle attack on social robots	PS10
Gaining and escalating super privileges through insider attack	PS13
Modifying data	
Modifying Pepper root password	PS01
Maliciously falsifying social robot cloud data	PS09
Tampering of social robot's data-in-use located in DRAM memory due to insider attack privilege escalation	PS13
Pepper social robot being accessed and misused by adversaries through insecure cloud-based interaction	PSA01
Instances of cyber criminals exploiting robotic platforms to modify data	PSA03
Read (Take/Steal) data	
Stealing Pepper's credentials and data	PS01
Leakage of users' identity data in the cloud	PS09
Stealing and tampering of data resulting from root users' privilege escalation	PS13
Access to Pepper through its connection to the Internet and cloud services	PSA01
Cyber criminals exploiting robotic platforms and stealing data	PSA03
Execute unauthorized commands	
Executing an arbitrary malicious code in Pepper through a MIME-sniffing attack	PS01
Injecting malevolent data and commands to the social robot while exploiting ROS vulnerabilities	PS13
Adversaries using malicious pdf attachments as an efficient weapon for executing codes in social robots	PSA04
Deny/Disrupt services or operation	
Publishing huge amounts of data to realize a DoS attack after a successful insider attack	PS13
Flooding communication network with heavy traffic to result in a DDoS attack	PSA03
Damage/Destroy assets or properties	
Damage to assets and reputation of an organization or individual	PS04
Causing damages in users' homes	PS13
Physical damage to museum's valuable artifacts and other assets	PSA01

Table A8. List of attacks identified in the primary studies.

IDs	Reported Attack	Attack Category
PS01	ARP Spoofing	Cyber
PS10	Botnet Attack	Cyber
PS13	Buffer overflow	Cyber
PS01	Clickjacking attacks	Cyber
PS13	Code injection attack	Cyber
PS13	Code-reuse attack	Cyber
PS13	Cold boot attack	Cyber
PS06	Collision resistance attack	Cyber
PS05	Damage to property	Environment
PS09	Data leakage	Cyber
PS09	Data modification	Cyber
PS10	Data sniffing attack	Cyber
PS04	Data Theft	Cyber
PS10	DDoS attack	Cyber

Table A8. *Cont.*

IDs	Reported Attack	Attack Category
PS11	Deception	Social,
PSA03	Denial of Service (DoS) attack	Cyber
PS13	DoS	Cyber
PS13	Eavesdropping	Cyber
PSA06	Embarrassment and privacy violation	Physical
PSA04	Embedded file attack	Cyber
PS11	Espionage (recording video, taking pictures and conducting searches on users)	Cyber
PS11	Exploiting human emotion	Social, Cyber
PSA05	Exploiting human trust towards social robots	Physical
PSA04	Form submission and URI attacks	Cyber
PSA01	GPS sensor attacks	Cyber
PS10	Hacking of Control Software	Cyber
PS05	Hacking	Cyber
PS09	Hacking	Cyber
PS11	Hacking	Cyber
PS08	Harm to humans resulting from robot failure	Physical
PSA05	Human factor attacks	Physical
PS12	Illegal authorization attacks	Cyber
PS07	Information theft (Espionage)	Cyber
PS05	Information theft	Cyber
PS03	Invading personal space	Social
PS13	Lago attack	Cyber
PS01	Malicious code execution	Cyber
PSA03	Malicious code execution	Cyber
PSA04	Malicious code execution	Cyber
PSA03	Malware attack	Cyber
PS01	Malware attack	Cyber
PS07	Malware attack	Cyber
PSA04	Malware attack	Cyber
PS07	Malware attack	Cyber
PS01	Man-in-the-Middle Attack	Cyber
PS10	Man-in-the-Middle Attack	Cyber
PS13	Man-in-the-Middle Attack	Cyber
PSA03	Man-in-the-Middle Attack	Cyber
PS11	Manipulation tactics	Cyber, Social
PS01	Meltdown and specter attacks	Cyber
PS01	MIME-sniffing attack	Cyber
PS13	Modifying Linux base attack	Cyber
PSA04	pdf file attacks	Cyber
PS11	Personal information extraction	Cyber
PS05	Personal space violation	Social
PS05	Phishing attacks (accounts and medical records)	Cyber
PS11	Phishing attacks	Cyber
PSA02	Physical (Harm to robot)	Physical
PSA02	Physical (Obstructing robot path)	Physical
PSA07	Physical (Obstructing robot path)	Physical
PSB01	Physical (Obstructing robot path)	Physical
PSA02	Physical (Psychological effects on humans)	Physical
PS02	Physical abuse (Physical violence towards robot)	Physical
PS13	Physical attacks that unpackage the CPU or any programming bug	Cyber
PSA01	Physical damage to properties/environment	Environment
PS01	Physical harm to human	Physical
PS13	Physical harm to human	Physical
PSA01	Physical harm to human	Physical
PSA03	Physical harm to human	Physical
PSA01	Psychological harm to human	Physical

Table A8. *Cont.*

IDs	Reported Attack	Attack Category
PS04	Remote Code Execution	Cyber
PSA03	Remote Control Without Authentication	Cyber
PS01	Remote Control Without Authentication	Cyber
PS13	Replay	Cyber
PSA07	Robot bullying	Physical
PSA07	Robot mistreatment	Physical
PSA07	Robot vandalism	Physical
PSA07	Sabotaging robot tasks	Physical
PS13	Side-channel attack	Cyber
PS13	Sniffing (bus-sniffing attack)	Cyber
PS07	Social engineering	Cyber
PS13	Specter attack	Cyber
PS04	Spoofing attack on user information	Cyber
PS01	SSH dictionary brute-force attack	Cyber
PS13	Stealing security certificates	Cyber
PS07	Surveillance	Cyber, Social
PSA06	Surveillance	Cyber, Social
PS05	Surveillance	Cyber
PS11	Theft (Stealing)	Physical, Social
PS05	Theft	Physical
PS02	Traffic analysis attack	Cyber
PS11	Trust violation	Social
PS05	User preference violation through targeted marketing	Cyber
PS02	Verbal abuse towards a robot	Physical
PSA07	Verbal violence towards robots	Physical
PS01	XSS (Cross-site scripting)	Cyber

Table A9. List of proposed attack mitigation reported in this study.

IDs	Attack	Attack Mitigation
PS01	Port Scanning attack	Use of Portspoof software and running of automated assessment tools
PS01	Security patches and updates-related attacks	Software security analysis and updates
PS01	Insecure communication channel with HTTP-related attacks	Communication over secure channels using HTTPS
PS01	Insecure-password-management-related attacks	Smarter access control mechanisms using blockchain smart contracts
PS01	Brute-force password attacks	IP blacklisting and setting upper bound for simultaneous connections
PS01	Unverified inputs resulting in malicious code execution	Adequate input validation
PS01	Man-in-the-Middle attacks	Secure cryptographic certificate handling
PS01	Remote control without authentication	Secure API design
PS02	Robot physical abuse by humans	Bystander intervention and possible social robot shutdown during abuse
PS03	Personal space invasion by social robots	Use of audible sound when making an approach
PS04	Anomalous behaviors in robots resulting from cyber-attacks	Intrusion detection and protection mechanism using system logs
PS04	Attacks resulting from insecure policies in robot development	Awareness and enforcing strong security policies
PS06	Data privacy violation in social robots	The use of BlockRobot with DAP based on EOS Blockchain
PS07	Recording of users' sensitive data (nakedness)	Automatic nakedness detection and prevention in smart homes using CNN
PS08	Physical harm to humans due to failure	Dynamic Social Zone (DSZ) framework

Table A9. *Cont.*

IDs	Attack	Attack Mitigation
PS09	Attacks resulting from identity authentication limitations	A secure identity authentication mechanism
PS09	Access-control-limitations-related attacks	A polynomial-based access control system
PS09	Attacks exploiting communication payload size and delay	An efficient security policy
PS10	Cyber-attacks on socially assistive robots	Secure IoT platform
PS12	Face visual privacy violation	Facial privacy generative adversarial network (FPGAN) model
PS13	An insider with root-privileges-related attack	Hardware-assisted trusted execution environment (HTEE)
PS13	Protection against return-oriented programming (ROP)	Isolation feature of hardware-assisted trusted execution environment (HTEE)
PSA01	Robot software development/testing vulnerabilities	Robot application security process platform in collaboration with security engineer
PSA02	Social robot abuse by children	A planning technique for avoiding children abuse
PSA03	Cyber and physical attacks on robotic platforms	A platform for monitoring and detection of attacks
PSA03	Public-space-factors-related attacks	Platform with alerts for fire, safety, water, power, and local news.
PSA04	Malicious code execution from pdf file access	Mobile malicious pdf detector (MMPD) algorithm
PSA06	Recording of privacy-sensitive images of users	A Real-time Object Detection Algorithm based on Feature YOLO (RODA-FY)
PSB01	Robot abuse by children	Recommended early stopping of abusive behaviors and preventing children from imitating abusive behaviors

References

1. Sheridan, T.B. A Review of Recent Research in Social Robotics. *Curr. Opin. Psychol.* **2020**, *36*, 7–12. [CrossRef] [PubMed]
2. Martinez-Martin, E.; Costa, A. Assistive Technology for Elderly Care: An Overview. *IEEE Access Pract. Innov. Open Solut.* **2021**, *9*, 92420–92430. [CrossRef]
3. Portugal, D.; Alvito, P.; Christodoulou, E.; Samaras, G.; Dias, J. A Study on the Deployment of a Service Robot in an Elderly Care Center. *Int. J. Soc. Robot.* **2019**, *11*, 317–341. [CrossRef]
4. Kyrarini, M.; Lygerakis, F.; Rajavenkatanarayanan, A.; Sevastopoulos, C.; Nambiappan, H.R.; Chaitanya, K.K.; Babu, A.R.; Mathew, J.; Makedon, F. A Survey of Robots in Healthcare. *Technologies* **2021**, *9*, 8. [CrossRef]
5. Logan, D.E.; Breazeal, C.; Goodwin, M.S.; Jeong, S.; O'Connell, B.; Smith-Freedman, D.; Heathers, J.; Weinstock, P. Social Robots for Hospitalized Children. *Pediatrics* **2019**, *144*, e20181511. [CrossRef]
6. Scoglio, A.A.; Reilly, E.D.; Gorman, J.A.; Drebing, C.E. Use of Social Robots in Mental Health and Well-Being Research: Systematic Review. *J. Med. Internet Res.* **2019**, *21*, e13322. [CrossRef]
7. Gerłowska, J.; Furtak-Niczyporuk, M.; Rejdak, K. Robotic Assistance for People with Dementia: A Viable Option for the Future? *Expert Rev. Med. Devices* **2020**, *17*, 507–518. [CrossRef]
8. Ghafurian, M.; Hoey, J.; Dautenhahn, K. Social Robots for the Care of Persons with Dementia: A Systematic Review. *ACM Trans. Hum.-Robot Interact.* **2021**, *10*, 1–31. [CrossRef]
9. Woods, D.; Yuan, F.; Jao, Y.-L.; Zhao, X. Social Robots for Older Adults with Dementia: A Narrative Review on Challenges & Future Directions. In Proceedings of the Social Robotics, Singapore, 2 November 2021; Li, H., Ge, S.S., Wu, Y., Wykowska, A., He, H., Liu, X., Li, D., Perez-Osorio, J., Eds.; Springer International Publishing: Cham, Germany, 2021; pp. 411–420.
10. Alam, A. Social Robots in Education for Long-Term Human-Robot Interaction: Socially Supportive Behaviour of Robotic Tutor for Creating Robo-Tangible Learning Environment in a Guided Discovery Learning Interaction. *ECS Trans.* **2022**, *107*, 12389. [CrossRef]
11. Belpaeme, T.; Kennedy, J.; Ramachandran, A.; Scassellati, B.; Tanaka, F. Social Robots for Education: A Review. *Sci. Robot.* **2018**, *3*, eaat5954. [CrossRef]
12. Lytridis, C.; Bazinas, C.; Sidiropoulos, G.; Papakostas, G.A.; Kaburlasos, V.G.; Nikopoulou, V.-A.; Holeva, V.; Evangeliou, A. Distance Special Education Delivery by Social Robots. *Electronics* **2020**, *9*, 1034. [CrossRef]
13. Rosenberg-Kima, R.B.; Koren, Y.; Gordon, G. Robot-Supported Collaborative Learning (RSCL): Social Robots as Teaching Assistants for Higher Education Small Group Facilitation. *Front. Robot. AI* **2020**, *6*, 148. [CrossRef]
14. Belpaeme, T.; Vogt, P.; van den Berghe, R.; Bergmann, K.; Göksun, T.; de Haas, M.; Kanero, J.; Kennedy, J.; Küntay, A.C.; Oudgenoeg-Paz, O.; et al. Guidelines for Designing Social Robots as Second Language Tutors. *Int. J. Soc. Robot.* **2018**, *10*, 325–341. [CrossRef] [PubMed]

15. Engwall, O.; Lopes, J.; Åhlund, A. Robot Interaction Styles for Conversation Practice in Second Language Learning. *Int. J. Soc. Robot.* **2021**, *13*, 251–276. [CrossRef]
16. Kanero, J.; Geçkin, V.; Oranç, C.; Mamus, E.; Küntay, A.C.; Göksun, T. Social Robots for Early Language Learning: Current Evidence and Future Directions. *Child Dev. Perspect.* **2018**, *12*, 146–151. [CrossRef]
17. van den Berghe, R.; Verhagen, J.; Oudgenoeg-Paz, O.; van der Ven, S.; Leseman, P. Social Robots for Language Learning: A Review. *Rev. Educ. Res.* **2019**, *89*, 259–295. [CrossRef]
18. Aaltonen, I.; Arvola, A.; Heikkilä, P.; Lammi, H. Hello Pepper, May I Tickle You? Children's and Adults' Responses to an Entertainment Robot at a Shopping Mall. In Proceedings of the Companion of the 2017 ACM/IEEE International Conference on Human-Robot Interaction, Vienna, Austria, 6–9 March 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 53–54.
19. Čaić, M.; Mahr, D.; Oderkerken-Schröder, G. Value of Social Robots in Services: Social Cognition Perspective. *J. Serv. Mark.* **2019**, *33*, 463–478. [CrossRef]
20. Yeoman, I.; Mars, M. Robots, Men and Sex Tourism. *Futures* **2012**, *44*, 365–371. [CrossRef]
21. Pinillos, R.; Marcos, S.; Feliz, R.; Zalama, E.; Gómez-García-Bermejo, J. Long-Term Assessment of a Service Robot in a Hotel Environment. *Robot. Auton. Syst.* **2016**, *79*, 40–57. [CrossRef]
22. Ivanov, S.; Seyitoğlu, F.; Markova, M. Hotel Managers' Perceptions towards the Use of Robots: A Mixed-Methods Approach. *Inf. Technol. Tour.* **2020**, *22*, 505–535. [CrossRef]
23. Mubin, O.; Ahmad, M.I.; Kaur, S.; Shi, W.; Khan, A. Social Robots in Public Spaces: A Meta-Review. In Proceedings of the Social Robotics, Qingdao, China, 27 November 2018; Ge, S.S., Cabibihan, J.-J., Salichs, M.A., Broadbent, E., He, H., Wagner, A.R., Castro-González, Á., Eds.; Springer International Publishing: Cham, Germany, 2018; pp. 213–220.
24. Thunberg, S.; Ziemke, T. Are People Ready for Social Robots in Public Spaces? In Proceedings of the Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction, Cambridge, UK, 23–26 March 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 482–484.
25. Mintrom, M.; Sumartojo, S.; Kulić, D.; Tian, L.; Carreno-Medrano, P.; Allen, A. Robots in Public Spaces: Implications for Policy Design. *Policy Des. Pract.* **2022**, *5*, 123–139. [CrossRef]
26. Radanliev, P.; De Roure, D.; Walton, R.; Van Kleek, M.; Montalvo, R.M.; Santos, O.; Maddox, L.; Cannady, S. COVID-19 What Have We Learned? The Rise of Social Machines and Connected Devices in Pandemic Management Following the Concepts of Predictive, Preventive and Personalized Medicine. *EPMA J.* **2020**, *11*, 311–332. [CrossRef] [PubMed]
27. Shen, Y.; Guo, D.; Long, F.; Mateos, L.A.; Ding, H.; Xiu, Z.; Hellman, R.B.; King, A.; Chen, S.; Zhang, C.; et al. Robots Under COVID-19 Pandemic: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 1590–1615. [CrossRef] [PubMed]
28. Research and Markets Global Social Robots Market—Growth, Trends, COVID-19 Impact, and Forecasts (2022–2027). Available online: https://www.researchandmarkets.com/reports/5120156/global-social-robots-market-growth-trends (accessed on 16 October 2022).
29. European Partnership on Artificial Intelligence, Data and Robotics AI Data Robotics Partnership EU. Available online: https://ai-data-robotics-partnership.eu/ (accessed on 15 October 2022).
30. United Nations ESCAP Ageing Societies. Available online: https://www.unescap.org/our-work/social-development/ageing-societies (accessed on 16 October 2022).
31. WHO Ageing and Health. Available online: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health (accessed on 16 October 2022).
32. Stone, R.; Harahan, M.F. Improving The Long-Term Care Workforce Serving Older Adults. *Health Aff.* **2010**, *29*, 109–115. [CrossRef]
33. Fosch Villaronga, E.; Golia, A.J. Robots, Standards and the Law: Rivalries between Private Standards and Public Policymaking for Robot Governance. *Comput. Law Secur. Rev.* **2019**, *35*, 129–144. [CrossRef]
34. Fosch-Villaronga, E.; Mahler, T. Cybersecurity, Safety and Robots: Strengthening the Link between Cybersecurity and Safety in the Context of Care Robots. *Comput. Law Secur. Rev.* **2021**, *41*, 105528. [CrossRef]
35. Fosch-Villaronga, E.; Lutz, C.; Tamò-Larrieux, A. Gathering Expert Opinions for Social Robots' Ethical, Legal, and Societal Concerns: Findings from Four International Workshops. *Int. J. Soc. Robot.* **2020**, *12*, 441–458. [CrossRef]
36. Chatterjee, S.; Chaudhuri, R.; Vrontis, D. Usage Intention of Social Robots for Domestic Purpose: From Security, Privacy, and Legal Perspectives. *Inf. Syst. Front.* **2021**, 1–16. [CrossRef]
37. Salvini, P.; Paez-Granados, D.; Billard, A. On the Safety of Mobile Robots Serving in Public Spaces: Identifying Gaps in EN ISO 13482:2014 and Calling for a New Standard. *ACM Trans. Hum.-Robot Interact.* **2021**, *10*, 1–27. [CrossRef]
38. Ahmad Yousef, K.M.; AlMajali, A.; Ghalyon, S.A.; Dweik, W.; Mohd, B.J. Analyzing Cyber-Physical Threats on Robotic Platforms. *Sensors* **2018**, *18*, 1643. [CrossRef]
39. Özdol, B.; Köseler, E.; Alçiçek, E.; Cesur, S.E.; Aydemir, P.J.; Bahtiyar, Ş. A Survey on Security Attacks with Remote Ground Robots. *El-Cezeri* **2021**, *8*, 1286–1308. [CrossRef]
40. Choi, J. Range Sensors: Ultrasonic Sensors, Kinect, and LiDAR. In *Humanoid Robotics: A Reference*; Goswami, A., Vadakkepat, P., Eds.; Springer: Dordrecht, The Netherlands, 2019; pp. 2521–2538. ISBN 978-94-007-6045-5.
41. Milella, A.; Reina, G.; Nielsen, M. A Multi-Sensor Robotic Platform for Ground Mapping and Estimation beyond the Visible Spectrum. *Precis. Agric.* **2019**, *20*, 423–444. [CrossRef]

42. Nandhini, C.; Murmu, A.; Doriya, R. Study and Analysis of Cloud-Based Robotics Framework. In Proceedings of the 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, India, 8–9 September 2017; pp. 800–8111.
43. Sun, Y. Cloud Edge Computing for Socialization Robot Based on Intelligent Data Envelopment. *Comput. Electr. Eng.* **2021**, *92*, 107136. [CrossRef]
44. Jawhar, I.; Mohamed, N.; Al-Jaroodi, J. Secure Communication in Multi-Robot Systems. In Proceedings of the 2020 IEEE Systems Security Symposium (SSS), Crystal City, VA, USA, 1 July–1 August 2020; pp. 1–8.
45. Bures, M.; Klima, M.; Rechtberger, V.; Ahmed, B.S.; Hindy, H.; Bellekens, X. Review of Specific Features and Challenges in the Current Internet of Things Systems Impacting Their Security and Reliability. In Proceedings of the Trends and Applications in Information Systems and Technologies, Terceira Island, Azores, Portugal, 30 March–2 April 2021; Rocha, Á., Adeli, H., Dzemyda, G., Moreira, F., Ramalho Correia, A.M., Eds.; Springer International Publishing: Cham, Germany, 2021; pp. 546–556.
46. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
47. Morales, C.G.; Carter, E.J.; Tan, X.Z.; Steinfeld, A. Interaction Needs and Opportunities for Failing Robots. In Proceedings of the 2019 on Designing Interactive Systems Conference, San Diego, CA, USA, 23–28 June 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 659–670.
48. Sailio, M.; Latvala, O.-M.; Szanto, A. Cyber Threat Actors for the Factory of the Future. *Appl. Sci.* **2020**, *10*, 4334. [CrossRef]
49. Liu, Y.-C.; Bianchin, G.; Pasqualetti, F. Secure Trajectory Planning against Undetectable Spoofing Attacks. *Automatica* **2020**, *112*, 108655. [CrossRef]
50. Tsiostas, D.; Kittes, G.; Chouliaras, N.; Kantzavelou, I.; Maglaras, L.; Douligeris, C.; Vlachos, V. The Insider Threat: Reasons, Effects and Mitigation Techniques. In Proceedings of the 24th Pan-Hellenic Conference on Informatics, Athens, Greece, 20–22 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 340–345.
51. Kaloudi, N.; Li, J. The AI-Based Cyber Threat Landscape: A Survey. *ACM Comput. Surv.* **2020**, *53*, 1–34. [CrossRef]
52. Boada, J.P.; Maestre, B.R.; Genís, C.T. The Ethical Issues of Social Assistive Robotics: A Critical Literature Review. *Technol. Soc.* **2021**, *67*, 101726. [CrossRef]
53. Sarrica, M.; Brondi, S.; Fortunati, L. How Many Facets Does a "Social Robot" Have? A Review of Scientific and Popular Definitions Online. *Inf. Technol. People* **2019**, *33*, 1–21. [CrossRef]
54. Henschel, A.; Laban, G.; Cross, E.S. What Makes a Robot Social? A Review of Social Robots from Science Fiction to a Home or Hospital Near You. *Curr. Robot. Rep.* **2021**, *2*, 9–19. [CrossRef]
55. Woo, H.; LeTendre, G.K.; Pham-Shouse, T.; Xiong, Y. The Use of Social Robots in Classrooms: A Review of Field-Based Studies. *Educ. Res. Rev.* **2021**, *33*, 100388. [CrossRef]
56. Papadopoulos, I.; Lazzarino, R.; Miah, S.; Weaver, T.; Thomas, B.; Koulouglioti, C. A Systematic Review of the Literature Regarding Socially Assistive Robots in Pre-Tertiary Education. *Comput. Educ.* **2020**, *155*, 103924. [CrossRef]
57. Donnermann, M.; Schaper, P.; Lugrin, B. Social Robots in Applied Settings: A Long-Term Study on Adaptive Robotic Tutors in Higher Education. *Front. Robot. AI* **2022**, *9*, 831633. [CrossRef] [PubMed]
58. Cooper, S.; Di Fava, A.; Villacañas, Ó.; Silva, T.; Fernandez-Carbajales, V.; Unzueta, L.; Serras, M.; Marchionni, L.; Ferro, F. Social Robotic Application to Support Active and Healthy Ageing. In Proceedings of the 2021 30th IEEE International Conference on Robot & Human Interactive Communication (RO-MAN), Vancouver, BC, Canada, 8–12 August 2021; pp. 1074–1080.
59. Mavroeidis, V.; Hohimer, R.; Casey, T.; Jesang, A. Threat Actor Type Inference and Characterization within Cyber Threat Intelligence. In Proceedings of the 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 25–28 May 2021; pp. 327–352.
60. Siva Kumar, R.S.; O'Brien, D.; Albert, K.; Viljoen, S.; Snover, J. Failure Modes in Machine Learning Systems. Available online: https://arxiv.org/abs/1911.11034 (accessed on 5 December 2022).
61. Giaretta, A.; De Donno, M.; Dragoni, N. Adding Salt to Pepper: A Structured Security Assessment over a Humanoid Robot. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg Germany, 27–30 August 2018; Association for Computing Machinery: New York, NY, USA, 2018.
62. Srinivas Aditya, U.S.P.; Singh, R.; Singh, P.K.; Kalla, A. A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions. *J. Netw. Comput. Appl.* **2021**, *196*, 103245. [CrossRef]
63. Dario, P.; Laschi, C.; Guglielmelli, E. Sensors and Actuators for "humanoid" Robots. *Adv. Robot.* **1996**, *11*, 567–584. [CrossRef]
64. Woodford, C. Robots. Available online: http://www.explainthatstuff.com/robots.html (accessed on 4 November 2022).
65. Tonkin, M.V. Socially Responsible Design for Social Robots in Public Spaces. Ph.D. Thesis, University of Technology Sydney, Sydney, Australia, 2021.
66. Fortunati, L.; Cavallo, F.; Sarrica, M. The Role of Social Robots in Public Space. In Proceedings of the Ambient Assisted Living, London, UK, 25 March 2019; Casiddu, N., Porfirione, C., Monteriù, A., Cavallo, F., Eds.; Springer International Publishing: Cham, Germany, 2019; pp. 171–186.
67. Altman, I.; Zube, E.H. *Public Places and Spaces*; Springer Science & Business Media: Berlin, Germany, 2012; ISBN 978-1-4684-5601-1.
68. Ross, R.; McEvilley, M.; Carrier Oren, J. *System Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*; NIST: Gaithersburg, MD, USA, 2016; p. 260.

69. Newhouse, W.; Johnson, B.; Kinling, S.; Kuruvilla, J.; Mulugeta, B.; Sandlin, K. *Multifactor Authentication for E-Commerce Risk-Based, FIDO Universal Second Factor Implementations for Purchasers*; NIST Special Publication 1800-17; NIST: Gaithersburg, MD, USA, 2019.
70. MITRE Common Attack Pattern Enumeration and Classification (CAPEC): Domains of Attack (Version 3.7). Available online: https://capec.mitre.org/data/definitions/3000.html (accessed on 19 September 2022).
71. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. *Int. J. Inf. Secur.* **2022**, *21*, 115–158. [CrossRef]
72. DeMarinis, N.; Tellex, S.; Kemerlis, V.P.; Konidaris, G.; Fonseca, R. Scanning the Internet for ROS: A View of Security in Robotics Research. In Proceedings of the 2019 International Conference on Robotics and Automation (ICRA), Montreal, QC, Canada, 20–24 May 2019; pp. 8514–8521.
73. Montasari, R.; Hill, R.; Parkinson, S.; Daneshkhah, A.; Hosseinian-Far, A. Hardware-Based Cyber Threats: Attack Vectors and Defence Techniques. *Int. J. Electron. Secur. Digit. Forensics* **2020**, *12*, 397–411. [CrossRef]
74. NIST. *Minimum Security Requirements for Federal Information and Information Systems*; NIST: Gaithersburg, MD, USA, 2006.
75. Barnard-Wills, D.; Marinos, L.; Portesi, S. *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*; European Union Agency for Network and Information Security: Athens, Greece, 2014; p. 62. ISBN 978-92-9204-096-3.
76. Dautenhahn, K. Methodology & Themes of Human-Robot Interaction: A Growing Research Field. *Int. J. Adv. Robot. Syst.* **2007**, *4*, 15. [CrossRef]
77. Baxter, P.; Kennedy, J.; Senft, E.; Lemaignan, S.; Belpaeme, T. From Characterising Three Years of HRI to Methodology and Reporting Recommendations. In Proceedings of the 2016 11th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Christchurch, New Zealand, 7–10 March 2016; pp. 391–398.
78. Höflich, J.R. Relationships to Social Robots: Towards a Triadic Analysis of Media-Oriented Behavior. *Intervalla* **2013**, *1*, 35–48.
79. Mayoral-Vilches, V. Robot Cybersecurity, a Review. *Int. J. Cyber Forensics Adv. Threats Investig.* 2021; *in press*.
80. Nieles, M.; Dempsey, K.; Pillitteri, V. *An Introduction to Information Security*; NIST Special Publication 800-12; NIST: Gaithersburg, MD, USA, 2017; Revision 1.
81. Alzubaidi, M.; Anbar, M.; Hanshi, S.M. Neighbor-Passive Monitoring Technique for Detecting Sinkhole Attacks in RPL Networks. In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, Jakarta, Indonesia, 5–7 December 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 173–182.
82. Shoukry, Y.; Martin, P.; Yona, Y.; Diggavi, S.; Srivastava, M. PyCRA: Physical Challenge-Response Authentication for Active Sensors under Spoofing Attacks. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 1004–1015.
83. Ross, R.; Pillitteri, V.; Dempsey, K.; Riddle; Guissanie, G. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*; NIST: Gaithersburg, MD, USA, 2020.
84. UK NCSS UK. National Cyber Security Strategy 2016–2021. 2016; p. 80. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed on 4 November 2022).
85. Ross, R.; Pillitteri, V.; Graubart, R.; Bodeau, D.; Mcquaid, R. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*; NIST Special Publication 800-160; NIST: Gaithersburg, MD, USA, 2021.
86. Lasota, P.A.; Song, T.; Shah, J.A. *A Survey of Methods for Safe Human-Robot Interaction*; Now Publishers: Delft, The Netherlands, 2017; ISBN 978-1-68083-279-2.
87. Garfinkel, S.L. *De-Identification of Personal Information*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015; p. NIST IR 8053.
88. Casey, T. Threat Agent Library Helps Identify Information Security Risks. *Intel Inf. Technol.* **2007**, *2*, 1–12. [CrossRef]
89. Zacharaki, A.; Kostavelis, I.; Gasteratos, A.; Dokas, I. Safety Bounds in Human Robot Interaction: A Survey. *Saf. Sci.* **2020**, *127*, 104667. [CrossRef]
90. Tian, L.; Oviatt, S. A Taxonomy of Social Errors in Human-Robot Interaction. *J. Hum.-Robot Interact.* **2021**, *10*, 1–32. [CrossRef]
91. Honig, S.; Oron-Gilad, T. Understanding and Resolving Failures in Human-Robot Interaction: Literature Review and Model Development. *Front. Psychol.* **2018**, *9*, 861. [CrossRef] [PubMed]
92. Cornelius, G.; Caire, P.; Hochgeschwender, N.; Olivares-Mendez, M.A.; Esteves-Verissimo, P.; Völp, M.; Voos, H. A Perspective of Security for Mobile Service Robots. In Proceedings of the ROBOT 2017: Third Iberian Robotics Conference, Seville, Spain, 22–24 November 2017; Ollero, A., Sanfeliu, A., Montano, L., Lau, N., Cardeira, C., Eds.; Springer International Publishing: Cham, Germany, 2018; pp. 88–100.
93. Cerrudo, C.; Apa, L. *Hacking Robots before Skynet*; IOActive: Seattle, WA, USA, 2017; pp. 1–17.
94. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2021: April 2020 to Mid July 2021*; Publications Office: Luxembourg, Luxembourg, 2021; ISBN 978-92-9204-536-4.
95. European Union Agency for Cybersecurity. *ENISA Cybersecurity Threat Landscape Methodology*; Publications Office: Luxembourg, Luxembourg, 2022.
96. Choo, K.-K.R. The Cyber Threat Landscape: Challenges and Future Research Directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
97. Kitchenham, B.; Brereton, P. A Systematic Review of Systematic Review Process Research in Software Engineering. *Inf. Softw. Technol.* **2013**, *55*, 2049–2075. [CrossRef]

98. Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
99. Oruma, S.O.; Sánchez-Gordón, M.; Colomo-Palacios, R.; Gkioulos, V.; Hansen, J. Supplementary Materials to "A Systematic Review of Social Robots in Public Spaces: Threat Landscape and Attack Surface"—Mendeley Data. *Mendeley Data* **2022**. [CrossRef]
100. Fong, T.; Nourbakhsh, I.; Dautenhahn, K. A Survey of Socially Interactive Robots. *Robot. Auton. Syst.* **2003**, *42*, 143–166. [CrossRef]
101. Mazzeo, G.; Staffa, M. TROS: Protecting Humanoids ROS from Privileged Attackers. *Int. J. Soc. Robot.* **2020**, *12*, 827–841. [CrossRef]
102. Felizardo, K.R.; Mendes, E.; Kalinowski, M.; Souza, É.F.; Vijaykumar, N.L. Using Forward Snowballing to Update Systematic Reviews in Software Engineering. In Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, Ciudad Real, Spain, 8–9 September 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 1–6.
103. Brščić, D.; Kidokoro, H.; Suehiro, Y.; Kanda, T. Escaping from Children's Abuse of Social Robots. In Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction, Portland, OR, USA, 2–5 March 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 59–66.
104. Lin, J.; Li, Y.; Yang, G. FPGAN: Face de-Identification Method with Generative Adversarial Networks for Social Robots. *Neural Netw.* **2021**, *133*, 132–147. [CrossRef]
105. Zhang, Y.; Qian, Y.; Wu, D.; Hossain, M.S.; Ghoneim, A.; Chen, M. Emotion-Aware Multimedia Systems Security. *IEEE Trans. Multimed.* **2019**, *21*, 617–624. [CrossRef]
106. Aroyo, A.M.; Rea, F.; Sandini, G.; Sciutti, A. Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble? *IEEE Robot. Autom. Lett.* **2018**, *3*, 3701–3708. [CrossRef]
107. Tan, X.Z.; Vázquez, M.; Carter, E.J.; Morales, C.G.; Steinfeld, A. Inducing Bystander Interventions During Robot Abuse with Social Mechanisms. In Proceedings of the 2018 ACM/IEEE International Conference on Human-Robot Interaction, Chicago, IL, USA, 5–8 March 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 169–177.
108. Yang, G.; Yang, J.; Sheng, W.; Junior, F.E.F.; Li, S. Convolutional Neural Network-Based Embarrassing Situation Detection under Camera for Social Robot in Smart Homes. *Sensors* **2018**, *18*, 1530. [CrossRef]
109. Fernandes, F.E.; Yang, G.; Do, H.M.; Sheng, W. Detection of Privacy-Sensitive Situations for Social Robots in Smart Homes. In Proceedings of the 2016 IEEE International Conference on Automation Science and Engineering (CASE), Fort Worth, TX, USA, 21–25 August 2016; pp. 727–732.
110. Bhardwaj, A.; Avasthi, V.; Goundar, S. Cyber Security Attacks on Robotic Platforms. *Netw. Secur.* **2019**, *2019*, 13–19. [CrossRef]
111. Truong, X.-T.; Yoong, V.N.; Ngo, T.-D. Dynamic Social Zone for Human Safety in Human-Robot Shared Workspaces. In Proceedings of the 2014 11th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI), Kuala Lumpur, Malaysia, 12–15 November 2014; pp. 391–396.
112. Krupp, M.M.; Rueben, M.; Grimm, C.M.; Smart, W.D. A Focus Group Study of Privacy Concerns about Telepresence Robots. In Proceedings of the 2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), Lisbon, Portugal, 28 August–1 September 2017; pp. 1451–1458.
113. Yamada, S.; Kanda, T.; Tomita, K. An Escalating Model of Children's Robot Abuse. In Proceedings of the 2020 15th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Cambridge, UK, 23–26 March 2020; pp. 191–199.
114. Olivato, M.; Cotugno, O.; Brigato, L.; Bloisi, D.; Farinelli, A.; Iocchi, L. A Comparative Analysis on the Use of Autoencoders for Robot Security Anomaly Detection. In Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Venetian Macao, Macau, 4–8 November 2019; pp. 984–989.
115. Vulpe, A.; Paikan, A.; Craciunescu, R.; Ziafati, P.; Kyriazakos, S.; Hemmer, A.; Badonnel, R. IoT Security Approaches in Social Robots for Ambient Assisted Living Scenarios. In Proceedings of the 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC), Lisbon, Portugal, 24–27 November 2019; pp. 1–6.
116. Abate, A.F.; Bisogni, C.; Cascone, L.; Castiglione, A.; Costabile, G.; Mercuri, I. Social Robot Interactions for Social Engineering: Opportunities and Open Issues. In Proceedings of the 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Online, 17–22 August 2020; pp. 539–547.
117. Hochgeschwender, N.; Cornelius, G.; Voos, H. Arguing Security of Autonomous Robots. In Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 3–8 November 2019; pp. 7791–7797.
118. Joosse, M.; Lohse, M.; Berkel, N.V.; Sardar, A.; Evers, V. Making Appearances: How Robots Should Approach People. *ACM Trans. Hum.-Robot Interact.* **2021**, *10*, 1–24. [CrossRef]
119. Vasylkovskyi, V.; Guerreiro, S.; Sequeira, J.S. BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Virtual Event, 2–6 November 2020; pp. 106–115.
120. Sanoubari, E.; Young, J.; Houston, A.; Dautenhahn, K. Can Robots Be Bullied? A Crowdsourced Feasibility Study for Using Social Robots in Anti-Bullying Interventions. In Proceedings of the 2021 30th IEEE International Conference on Robot & Human Interactive Communication (RO-MAN), Vancouver, BC, Canada, 8–12 August 2021; pp. 931–938.

121. Cui, Y.; Sun, Y.; Luo, J.; Huang, Y.; Zhou, Y.; Li, X. MMPD: A Novel Malicious PDF File Detector for Mobile Robots. *IEEE Sens. J.* **2020**, *1*, 17583–17592. [CrossRef]
122. Garousi, V.; Fernandes, J.M. Highly-Cited Papers in Software Engineering: The Top-100. *Inf. Softw. Technol.* **2016**, *71*, 108–128. [CrossRef]
123. Lockheed Martin Cyber Kill Chain®. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 6 June 2022).
124. MITRE CAPEC: Mechanisms of Attack. Available online: https://capec.mitre.org/data/definitions/1000.html (accessed on 29 September 2022).
125. IGI Global What Is Attack Scenario | IGI Global. Available online: https://www.igi-global.com/dictionary/attack-scenario/59726 (accessed on 2 October 2022).
126. ENISA Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. Available online: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving (accessed on 1 October 2022).
127. NIST NIST Cybersecurity Framework Version 1.1. Available online: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework (accessed on 6 June 2022).
128. Agrafiotis, I.; Nurse, J.R.C.; Goldsmith, M.; Creese, S.; Upton, D. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *J. Cybersecurity* **2018**, *4*, tyy006. [CrossRef]
129. Collins, E.C. Drawing Parallels in Human–Other Interactions: A Trans-Disciplinary Approach to Developing Human–Robot Interaction Methodologies. *Philos. Trans. R. Soc. B Biol. Sci.* **2019**, *374*, 20180433. [CrossRef] [PubMed]
130. Moon, M. SoftBank Reportedly Stopped the Production of Its Pepper Robots Last Year: The Robot Suffered from Weak Demand According to Reuters and Nikkei. Available online: https://www.engadget.com/softbank-stopped-production-pepper-robots-032616568.html (accessed on 8 October 2022).
131. Nocentini, O.; Fiorini, L.; Acerbi, G.; Sorrentino, A.; Mancioppi, G.; Cavallo, F. A Survey of Behavioral Models for Social Robots. *Robotics* **2019**, *8*, 54. [CrossRef]
132. Johal, W. Research Trends in Social Robots for Learning. *Curr. Robot. Rep.* **2020**, *1*, 75–83. [CrossRef]
133. Kirschgens, L.A.; Ugarte, I.Z.; Uriarte, E.G.; Rosas, A.M.; Vilches, V.M. Robot Hazards: From Safety to Security. *arXiv* **2021**, arXiv:1806.06681.
134. Wohlin, C.; Runeson, P.; Höst, M.; Ohlsson, M.C.; Regnell, B.; Wesslén, A. *Experimentation in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2012; ISBN 978-3-642-29043-5.
135. ENISA Threat Landscape for Supply Chain Attacks. Available online: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (accessed on 6 June 2022).
136. Mohamed Shaluf, I. Disaster Types. *Disaster Prev. Manag. Int. J.* **2007**, *16*, 704–717. [CrossRef]
137. Jbair, M.; Ahmad, B.; Maple, C.; Harrison, R. Threat Modelling for Industrial Cyber Physical Systems in the Era of Smart Manufacturing. *Comput. Ind.* **2022**, *137*, 103611. [CrossRef]
138. Li, H.; Liu, Q.; Zhang, J. A Survey of Hardware Trojan Threat and Defense. *Integration* **2016**, *55*, 426–437. [CrossRef]
139. Sidhu, S.; Mohd, B.J.; Hayajneh, T. Hardware Security in IoT Devices with Emphasis on Hardware Trojans. *J. Sens. Actuator Netw.* **2019**, *8*, 42. [CrossRef]
140. Tuma, K.; Calikli, G.; Scandariato, R. Threat Analysis of Software Systems: A Systematic Literature Review. *J. Syst. Softw.* **2018**, *144*, 275–294. [CrossRef]
141. Das, A.; Baki, S.; El Aassal, A.; Verma, R.; Dunbar, A. SoK: A Comprehensive Reexamination of Phishing Research From the Security Perspective. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 671–708. [CrossRef]
142. Choi, M.; Robles, R.J.; Hong, C.; Kim, T. Wireless Network Security: Vulnerabilities, Threats and Countermeasures. *Int. J. Multimed. Ubiquitous Eng.* **2008**, *3*, 10.
143. Stallings, W.; Brown, L. *Computer Security: Principles and Practice*, 4th ed.; Pearson: New York, NY, USA, 2018; ISBN 978-0-13-479410-5.
144. NIST; Jansen, W.; Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing*; NIST: Gaithersburg, MD, USA, 2011; p. 80.
145. Masahiko, O.; Nobuyuki, I.; Yuto, N.; Masayuki, I. Stiffness Readout in Musculo-Skeletal Humanoid Robot by Using Rotary Potentiometer. In Proceedings of the 2010 IEEE SENSORS, Waikoloa, HI, USA, 1–4 November 2010; pp. 2329–2333.
146. Lang, H.; Wang, Y.; de Silva, C.W. Mobile Robot Localization and Object Pose Estimation Using Optical Encoder, Vision and Laser Sensors. In Proceedings of the 2008 IEEE International Conference on Automation and Logistics, Qingdao, China, 1–3 September 2008; pp. 617–622.
147. Wang, Z.; Zhang, J. Calibration Method of Internal and External Parameters of Camera Wheel Tachometer Based on TagSLAM Framework. In Proceedings of the International Conference on Signal Processing and Communication Technology (SPCT 2021), Harbin, China, 23–25 December 2021; SPIE: Bellingham, WA, USA, 2022; Volume 12178, pp. 413–417.
148. Huang, Q.; Zhang, S. Applications of IMU in Humanoid Robot. In *Humanoid Robotics: A Reference*; Goswami, A., Vadakkepat, P., Eds.; Springer: Dordrecht, The Netherlands, 2017; pp. 1–23. ISBN 978-94-007-7194-9.
149. Ding, S.; Ouyang, X.; Liu, T.; Li, Z.; Yang, H. Gait Event Detection of a Lower Extremity Exoskeleton Robot by an Intelligent IMU. *IEEE Sens. J.* **2018**, *18*, 9728–9735. [CrossRef]
150. Kunal, K.; Arfianto, A.Z.; Poetro, J.E.; Waseel, F.; Atmoko, R.A. Accelerometer Implementation as Feedback on 5 Degree of Freedom Arm Robot. *J. Robot. Control JRC* **2020**, *1*, 31–34. [CrossRef]

151. Kim, H.W.; Jung, S. Design and Control of a Sphere Robot Using a Control Moment Gyroscope Actuator for Navigation. *Int. J. Control Autom. Syst.* **2020**, *18*, 3112–3120. [CrossRef]
152. Zhmud, V.A.; Kondratiev, N.O.; Kuznetsov, K.A.; Trubin, V.G.; Dimitrov, L.V. Application of Ultrasonic Sensor for Measuring Distances in Robotics. *J. Phys. Conf. Ser.* **2018**, *1015*, 032189. [CrossRef]
153. Liu, Y.; Fan, R.; Yu, B.; Bocus, M.J.; Liu, M.; Ni, H.; Fan, J.; Mao, S. Mobile Robot Localisation and Navigation Using LEGO NXT and Ultrasonic Sensor. In Proceedings of the 2018 IEEE International Conference on Robotics and Biomimetics (ROBIO), Kuala Lumpur, Malaysia, 12–15 December 2018; pp. 1088–1093.
154. Bagate, A.; Shah, M. Human Activity Recognition Using RGB-D Sensors. In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May 2019; pp. 902–905.
155. Sushrutha Raghavan, V.; Kanoulas, D.; Zhou, C.; Caldwell, D.G.; Tsagarakis, N.G. A Study on Low-Drift State Estimation for Humanoid Locomotion, Using LiDAR and Kinematic-Inertial Data Fusion. In Proceedings of the 2018 IEEE-RAS 18th International Conference on Humanoid Robots (Humanoids), Beijing, China, 6–9 November 2018; pp. 1–8.
156. Guo, H.; Pu, X.; Chen, J.; Meng, Y.; Yeh, M.-H.; Liu, G.; Tang, Q.; Chen, B.; Liu, D.; Qi, S.; et al. A Highly Sensitive, Self-Powered Triboelectric Auditory Sensor for Social Robotics and Hearing Aids. *Sci. Robot.* **2018**, *3*, eaat2516. [CrossRef]
157. Natale, L.; Cannata, G. Tactile Sensing. In *Humanoid Robotics: A Reference*; Goswami, A., Vadakkepat, P., Eds.; Springer: Dordrecht, The Netherlands, 2019; pp. 2539–2561. ISBN 978-94-007-6045-5.
158. Avelino, J.; Paulino, T.; Cardoso, C.; Nunes, R.; Moreno, P.; Bernardino, A. Towards Natural Handshakes for Social Robots: Human-Aware Hand Grasps Using Tactile Sensors. *Paladyn J. Behav. Robot.* **2018**, *9*, 221–234. [CrossRef]
159. Sun, Q.-J.; Zhao, X.-H.; Zhou, Y.; Yeung, C.-C.; Wu, W.; Venkatesh, S.; Xu, Z.-X.; Wylie, J.J.; Li, W.-J.; Roy, V.A.L. Fingertip-Skin-Inspired Highly Sensitive and Multifunctional Sensor with Hierarchically Structured Conductive Graphite/Polydimethylsiloxane Foams. *Adv. Funct. Mater.* **2019**, *29*, 1808829. [CrossRef]
160. Chi, C.; Sun, X.; Xue, N.; Li, T.; Liu, C. Recent Progress in Technologies for Tactile Sensors. *Sensors* **2018**, *18*, 948. [CrossRef]
161. Huang, G.; Chen, J.; Benesty, J.; Cohen, I.; Zhao, X. Steerable Differential Beamformers with Planar Microphone Arrays. *EURASIP J. Audio Speech Music Process.* **2020**, *2020*, 15. [CrossRef]
162. Karakaya, D.; Ulucan, O.; Turkan, M. A Comparative Study on Electronic Nose Data Analysis Tools. In Proceedings of the 2020 Innovations in Intelligent Systems and Applications Conference (ASYU), Istanbul, Turkey, 15–17 October 2020; pp. 1–5.
163. Eamsa-ard, T.; Seesaard, T.; Kerdcharoen, T. Wearable Sensor of Humanoid Robot-Based Textile Chemical Sensors for Odor Detection and Tracking. In Proceedings of the 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST), Phuket, Thailand, 4–7 July 2018; pp. 1–4.
164. Yoshimatsu, J.; Toko, K.; Tahara, Y.; Ishida, M.; Habara, M.; Ikezaki, H.; Kojima, H.; Ikegami, S.; Yoshida, M.; Uchida, T. Development of Taste Sensor to Detect Non-Charged Bitter Substances. *Sensors* **2020**, *20*, 3455. [CrossRef]
165. Guan, W.; Huang, L.; Hussain, B.; Yue, C.P. Robust Robotic Localization Using Visible Light Positioning and Inertial Fusion. *IEEE Sens. J.* **2022**, *22*, 4882–4892. [CrossRef]
166. Cheng, H.-T.; Yang, Y.-C.; Liu, T.-H.; Wu, C.-H. Recent Advances in 850 Nm VCSELs for High-Speed Interconnects. *Photonics* **2022**, *9*, 107. [CrossRef]
167. Bajpai, R.; Tiwari, A.; Jain, A.; Joshi, D. A Novel Instrumented Outsole for Real-Time Foot Kinematic Measurements: Validation Across Different Speeds and Simulated Foot Landing. *IEEE Trans. Instrum. Meas.* **2022**, *71*, 1–10. [CrossRef]
168. Zhang, Z. Path Planning of a Firefighting Robot Prototype Using GPS Navigation. In Proceedings of the 2020 3rd International Conference on Robot Systems and Applications, Chengdu, China, 14–16 June 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 16–20.
169. Qin, K.; Chen, C.; Pu, X.; Tang, Q.; He, W.; Liu, Y.; Zeng, Q.; Liu, G.; Guo, H.; Hu, C. Magnetic Array Assisted Triboelectric Nanogenerator Sensor for Real-Time Gesture Interaction. *Nano-Micro Lett.* **2021**, *13*, 51. [CrossRef] [PubMed]