healthcare

Viewpoint

The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives

Daniele Giansanti [1],* and Rosario Alfio Gulino [2]

[1] Centre Tisp, Istituto Superiore di Sanità, 00161 Rome, Italy
[2] Faculty of Engineering, Tor Vergata University, Via Cracovia, 00133 Roma, Italy; rosario.gulino.uni.tv@hotmail.com
* Correspondence: daniele.giansanti@iss.it; Tel.: +39-06-49902701

Abstract: Care robots represent an opportunity for the health domain. The use of these robots has important implications. They can be used in surgery, rehabilitation, assistance, therapy, and other medical fields. Therefore, care robots (CR)s, have both important physical and psychological implications during their use. Furthermore, these devices, meet important data in clinical applications. These data must be protected. Therefore, cybersecurity (CS) has become a crucial characteristic that concerns all the involved actors. The study investigated the collocation of CRs in the context of CS studies in the health domain. Problems and peculiarities of these devices, with reference to the CS, were faced, investigating in different scientific databases. Highlights, ranging also from ethics implications up to the regulatory legal framework (ensuring safety and cybersecurity) have been reported. Models and cyber-attacks applicable on the CRs have been identified.

Keywords: e-health; medical devices; m-health; rehabilitation; robotics; organization models; artificial intelligence; electronic surveys; social robots; collaborative robots; cyber security; cyber risk; informatics

check for updates

Citation: Giansanti, D.; Gulino, R.A. The Cybersecurity and the Care Robots: A Viewpoint on the Open Problems and the Perspectives. *Healthcare* **2021**, *9*, 1653. https://doi.org/10.3390/healthcare9121653

Academic Editor: Tin-Chih Toly Chen

Received: 5 November 2021
Accepted: 24 November 2021
Published: 29 November 2021

1. Introduction

The cybersecurity (CS) in healthcare deals with the cyber risks in the cyber-systems used in the *health domain*. These systems can be medical devices and/or a complex interoperable and heterogeneous systems (e.g., Radiology Information System) [1,2]. A frightening growth is expected in the sector of the care robots (CR)s. The applications of social robots [3,4], for example, are continuously increasing [5,6].

Hence, it is now very important to address CS in CRs.

The Policy Department for Economic, Scientific and Quality of Life Policies, of the European Parliament, identified the most interesting applications for the CRs [7]: *Robotic surgery, Care and Socially assistive Robots, Rehabilitation systems, Training for health and care workers*. The sector is wide, complex and with numerous implications for the CS. For example, the rehabilitation robotics [8] has three motion applications (Table 1):

1. The stability.
2. The lower limbs.
3. The upper limbs.

Furthermore, rehabilitation robots use two different technological solutions (exoskeleton technology and end-effector technology), with different implications for the CS.

Social robots (SR)s are used in several diversified fields of assistance and rehabilitation [3,4]. Similar considerations can be carried out for the other applications. The implications between technologies, applications and CS immediately emerge from the definition of CR. CRs are complex and interoperable systems [9]. The European Foresight Monitoring Network [10] defines the CR as a system "able to perform coordinated mechatronic actions (force or movement exertions) based on processing information acquired through sensor technology, to support the functioning of impaired individuals, medical interventions, care and rehabilitation of patients and also individuals in prevention programs".

Table 1. Classification of the rehabilitation robot according to the applications.

Application	Description
Upper limb rehabilitation	Allowing rehabilitation of the upper limb using exoskeletons or end-effector system
Lower limb rehabilitation	Allowing rehabilitation of the lower limb using exoskeletons or end-effector system
Stability	Allowing the stability training and recovery using exoskeletons or end-effector system

The European Parliament traced for the CR the direction of the CS, highlighting that (literally cited) "possible applications of AI and robotics in medical care (are) managing medical records and data, performing repetitive jobs (analysing tests, X-rays, CT scans, data entry), treatment design, digital consultation (such as medical consultation based on personal medical history and common medical knowledge), virtual nurses, medication management, drug creation, precision medicine (as genetics and genomics look for mutations and links to disease from the information in DNA), health monitoring and healthcare system analysis, among other." [11].

It is important to investigate the progress of CS studies on the CRs. It is also important to investigate the problems and peculiarities. Correlations with other disciplines are important, such as, for example, ethics and regulation.

CRs, in fact, have characteristics, that are not found on other devices. They can replace caregivers or provide psychological or motor rehabilitation. The implications of CS in a programming error or a sabotage are high. Traditional problems can be found. However, many others are added. Motor damage can occur. Psychological damage can occur. Think about the false relationship that can be created with a pet SR. Think about the problems that an incorrect programming of the ethics concepts of an SR can bring.

The objective of the study is:

(a) To investigate the positioning of CRs in CS studies.
(b) Analyse the problems and peculiarities of the devices that have an impact in this area.
(c) Take stock of the related issues of ethics and regulation.

In this paper the authors discuss the conception of a viewpoint, presented and explained in four sections (plus the introduction and conclusions).

The first section (paragraph 2: The position of the care robots in the studies) deals with the state of production of studies in this area. This is carried out through an analysis of the production of scientific literature. The second section (paragraph 3: Ethics, care robots and cybersecurity) deals with the impact of the ethical issues. In particular, the correlation of the CS both with the ethics of research and with the programming of ethics on CRs is highlighted. The third section (paragraph 4: Regulatory framework, care robots and cybersecurity) deals with the situation of the regulatory framework. The fourth section (paragraph 5: Cyber-attacks applicable to care robots) reports models and cyber-attacks.

2. The Position of the Care Robots in the Studies

We are certainly witnessing a growing interest in the CS.

A simple search on the Pubmed database, the most important database of the health domain, shows 12.785 results on the cyber security [12]. Among them, a group identified in [13] deals with robots. By expanding the search with the keys safety and risk we find:

4882 articles with the key (safety [Title/Abstract]) AND (robot) [14].

5005 articles with the key (risk [Title/Abstract]) AND (robot) [15].

Scientists refer to safety or risk also to address issues related to informatic faults/problems. These informatic problems/faults can affect the mechatronics, and therefore, the human interface. This is a CS issue. Certainly, this is a first important indication for scholars. The experience gained in the sector in the industry, production, and consuming sector (IPCS) is another important issue to consider. Here, the theme of the safety of robot-human interaction in the workplace is highly developed. Here, the topic has been dealt with for much longer. Safety in robots is addressed. However, the use of robots for security is also addressed. Both are CS related issues. Part of the experience gained here, can be exported and readapted in the health domain, a particular workplace. Presently [16], there are three categories of robots in the IPCS: (1) industrial robots; (2) professional and personal service robots, and (3) collaborative robots. Studies reporting recommendations are spreading for these types of robots [16,17]. Some studies are specifically dealing with physical security [18] also in relation to CS. Other studies are dealing with traditional issues, such as security and privacy issues [19].

Very interesting models dealt with the security in the workplace. The Advanced Human-Robot Collaboration Model (AHRCM) approach was proposed in [20]. The idea was to enhance the risk assessment and to improve the safety in the workplace. The experimental results showed that the proposed AHRCM model achieved high performance in human-robot collaboration to reduce the risk.

The recent review in [21] highlighted how CS experience in IPCS robotics is exportable to the world of CRs. The same authors highlighted models and types of cyber-attacks on the CRs. Recent studies dealt with the security with SRs [22]. This included: risk assessment of communications security, predictive analysis of security risks, implementing access control policies to enhance the security of solution, and auditing of the solution against security, safety and privacy guidelines and regulations. A limited approach to some issues of CS was addressed in a few studies, such as in surgical applications [23] or in the rehabilitation of the lower limbs [24].

Other studies showed a backwardness in importing into the health domain the experience made elsewhere [25]. Probably, this is due to the limits and inadequacy of legislation concerning the CS [9,26]. It is also very important to observe how scientific societies move around the CS theme.

For example, CS has now become an indispensable issue in the topic Human Computer Interaction (HCI), in international scientific meetings [27]. In fact, one of the most important international conferences on HCI, hosts a section (HCI-CPT: International Conference on HCI for Cybersecurity, Privacy and Trust) dedicated to the CS applied to HCI. This highlights the importance of the theme for machines that interface/integrate with the human. In [28], a work presented at the HCI-CPT, it is also highlighted how the analysis must be extended directly in the field (for example in the workplace), involving the insiders in targeted investigations, with dedicated surveys, to understand behaviours at risk, as regards CS.

It is also necessary to consider the peculiarities of the CRs.

The ethical implications for the CRs are much more relevant than for other categories of robots. It is also necessary to consider more risks and criticalities. These risks and criticalities affect not only the physical issues, but also the psychological issues [9].

It was proposed in [9] a model describing the relationships between cyber-attacks/software fault/AI deficit and the impact on human safety.

We specialize in Figure 1, the model in the case of rehabilitation and assistance robotics. This model highlights the health risks for the user.

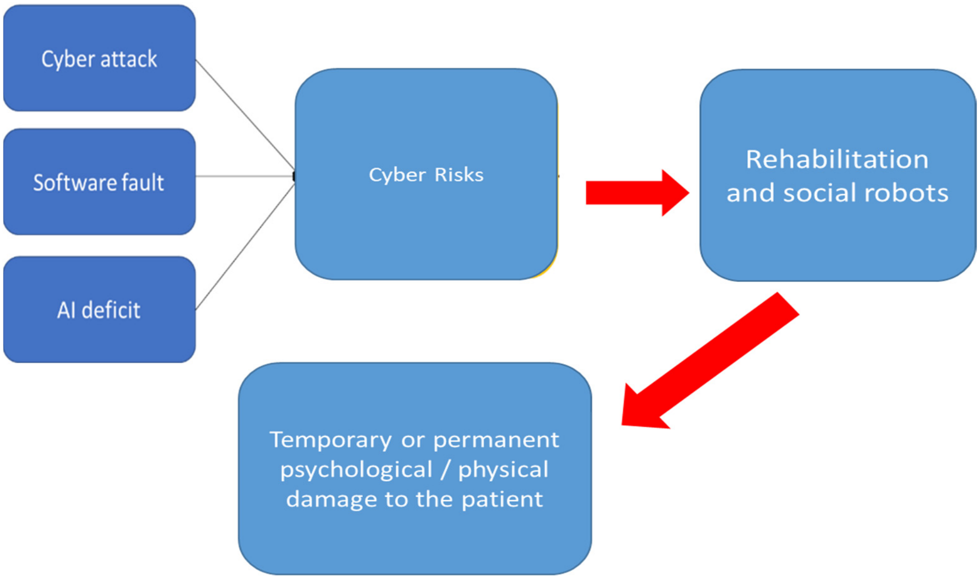

Cyber attack
Software fault
AI deficit
Cyber Risks
Rehabilitation and social robots
Temporary or permanent psychological / physical damage to the patient

Figure 1. Model of health risks for the CRs.

3. Ethics, Care Robots and Cybersecurity

Very important ethical discussions are open. A search on Pubmed with the key (social robot) AND (ethics) shows some interesting scientific contributes [29], confirming the wide discussion around the ethics. Ethics has a strong impact on the world of the CRs. This is reflected in the CS. We extended here the search also to other databases.

We can undoubtedly distinguish two important macro-sectors with an impact on CS. The first macro-sector is the ethics in a responsible research and innovation [30]. The second macro-sector is the ethics problem encountered while building moral CRs [31].

Stahl and Coeckelbergh highlighted, for the first macro-sector [30], that traditional approaches to the ethics of robotics are often distant from innovation practices and contexts of use. They listed in their review key concerns of ethics. As it has been highlighted in [30] there is a strong scientific production of ethics of CRs [32–39], or machine (medical) ethics [40–44] connected to the CRs. Three aspects were identified in [30].

First, there are important impacts both in the society and in the health domain:

Replacement and its implications for labour.

Replacement and its implications for the quality of care; they are the so-called de-humanisation and "cold" care.

Second, there are issues raised by human–robot interaction in the health domain and especially by the robot taking over tasks from humans, for instance: autonomy (connected to the implication of the robots take decision with autonomy) Role and tasks (connected to the changes in the workflow), Responsibility (connected to the responsibility chain in case of problems), The Deception (connected, for example, to the use of SRs as 'social companions, related to questions of opportunities and justification). Trust (connected, for example, to the reliability of giving subjects (also frail) in the hands of a CR.

Third, there are issues traditionally connected to the CS as for example:

Privacy and data protection.

Safety and avoidance of harm.

The second macro-sector [31] on the ethics problems is encountered while building moral CRs. It focuses on the interdisciplinary field of machine ethics—that is, how to program ethical rules and concepts inside on a robot [45]. This sector has become of utmost importance because the recent technological developments in the field of the CRs and artificial intelligence in general [46–50]. Gordon highlighted that to make ethics [31] "computable" (literally cited "depends in part, on how the designers understand ethics and attempt to implement that understanding in programs, but also more generally on their expertise in the field".

Based on the review [31] it was found that, scholars in the field in informatics applied to machine ethics have gaps in training and practical knowledge of ethics. There is therefore an important CS due to this.

From the previous analysis, a strong connection emerges between ethical issues and CS in the CRs. There is a strong need to rethink a more expanded CS also connected to the ethics in robotics.

4. Regulatory Framework, Care Robots and Cybersecurity

Surely when we consider the regulatory issues, we must ponder that CRs also use eHealth [51]. However, many other issues must be considered [9,26]. These issues range from the impact of mechatronics up to the use as a networked medical device. Some studies have highlighted lights and shadows of the regulatory framework [9], arranged in Europe into:

- Safety regulations [52].
- Legislation on medical devices (MD)s classification [53].
- Legal frameworks on the cybersecurity [54,55].

4.1. Care Robots and Safety Regulations

Robots, in general, and CRs, follow [52] the General Product Safety Directive (Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety 2001) and the Directive 85/374/EEC on liability for defective products. The applicability of product liability regulations is not easily and directly applicable in the context of robotics applications.

4.2. Care Robots and Medical Device Regulation

CRs, based on their destination of use, can be classified as a medical device (MD). The European Medical Device Regulation (Regulation (EU) 2017/745) [53] contains a detailed definition of MDs.

The Regulation contains three important actions (lights) in the direction of the CS concerning the minimization of the risks, the design of the software (including CS), the inclusion of the respect of a set of IT requirements also related to the CS.

The regulation [53] certainly presents great innovations for the CS. However, there are some shadows. The first shadow is that this regulation focuses a lot on manufacturers and little on recipients/users [9,26], who have a leading role. Perhaps, instruction sheets and manuals are not always enough. The second shadow [9,26] is that compliance with CS requirements is challenging, in part due to the potential overlap of different certification schemes with varying geographical or product scope and evolution of external regulations (see for example the Cybersecurity Act). The third shadow, we personally think applicable is that the intended use and certification must be aligned [8] and this it is not always easy to detect.

4.3. Care Robots and Regulations on the Cybersecurity

Three are the documents regarding the legal frameworks regulating CR CS [54–56]:

1. The directive on security of network and information systems (also called NIS Directive) that provides measures for boosting the overall CS in the EU [54].
2. The General Data Protection Regulation (GDPR) obligating to implement appropriate measures to ensure a level of security appropriate to relevant risks [55].
3. The EU Cyber-security Act (Regulation (EU) 2019/881) which establishes an EU-wide cybersecurity certification framework [57].

None of the documents has been specifically designed for CRs.

The first two documents [53,54] work in synergy.

According to the NIS Directive, operators need to respond appropriately to manage the CS in a network [9]. A Network can, (according to the NIS Directive [54]), include MDs, such as robots. As the healthcare providers also process personal data, they are, therefore, subject to the provisions of the GDPR [55].

The third document, the EU cybersecurity Act establishes a road map for voluntary CS certifications valid in the EU [56].

Among the evident limitations of the three documents [54–56] (in addition to the fact that they are not specifically designed for CRs) we find that: the first two delegate CS to healthcare providers, although they can be found on the market CRs with very different levels of CS [9]. The third document provides for a certification, but this is only voluntary.

5. Cyber-Attacks Applicable to Care Robots

CS for CRs must consider a broader spectrum of problems than other critical MDs, where, nevertheless, CS is more consolidated, such as the pacemakers [57–59] and the artificial pancreas [60–62]. CRs can generate, for example a psychological harm (Figure 1). This is also a consequence of issues dealt in par. 3 [30,31]. Much of the experience in robotics [16–20] on physiological harms/damages can be exported to CRs. Indeed, in [21] a process of unification has been carried out, which has general validity. Figure 2 summarizes the different robot-related threats, their causes, and their consequences in the case of the CRs. With reference to the figure, the nature of the attack is: internal vs external, coordinated vs random, detected/undetected, corrected/uncorrected. The identification is: data confidentiality and privacy, message authentication, device/user authentication, system integrity, data availability, system availability. The target is: the application layer, the hardware layer, the firmware layer. The impact can be low, moderate, high. The trust and safety concerns (according to the model in paragraph 2) are data integrity and privacy, physical harm, physical damage, psychological harm.

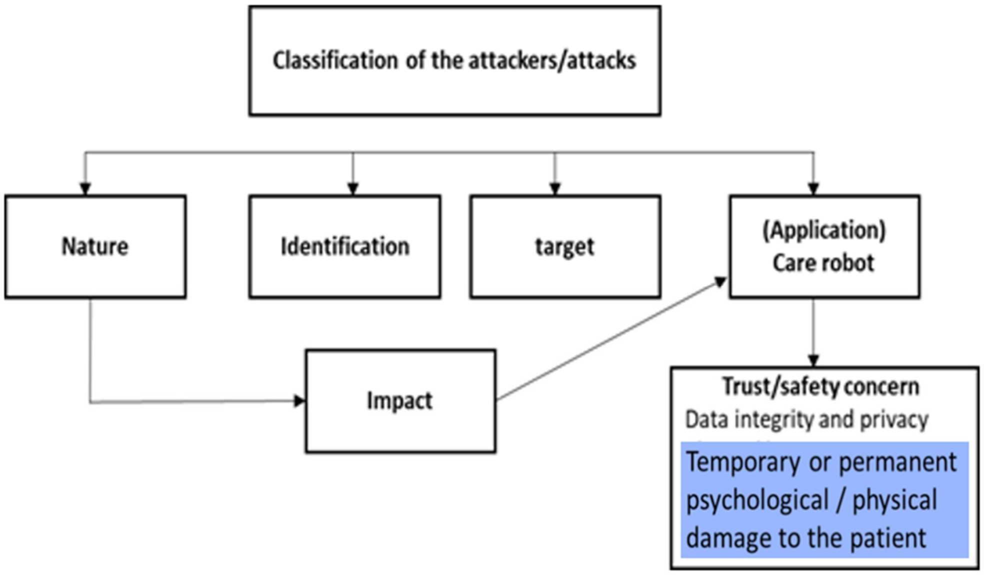

Classification of the attackers/attacks
Nature
Identification
target
(Application) Care robot
Impact
Trust/safety concern
Data integrity and privacy
Temporary or permanent psychological / physical damage to the patient

Figure 2. Model of robot-related threats, causes, and consequences.

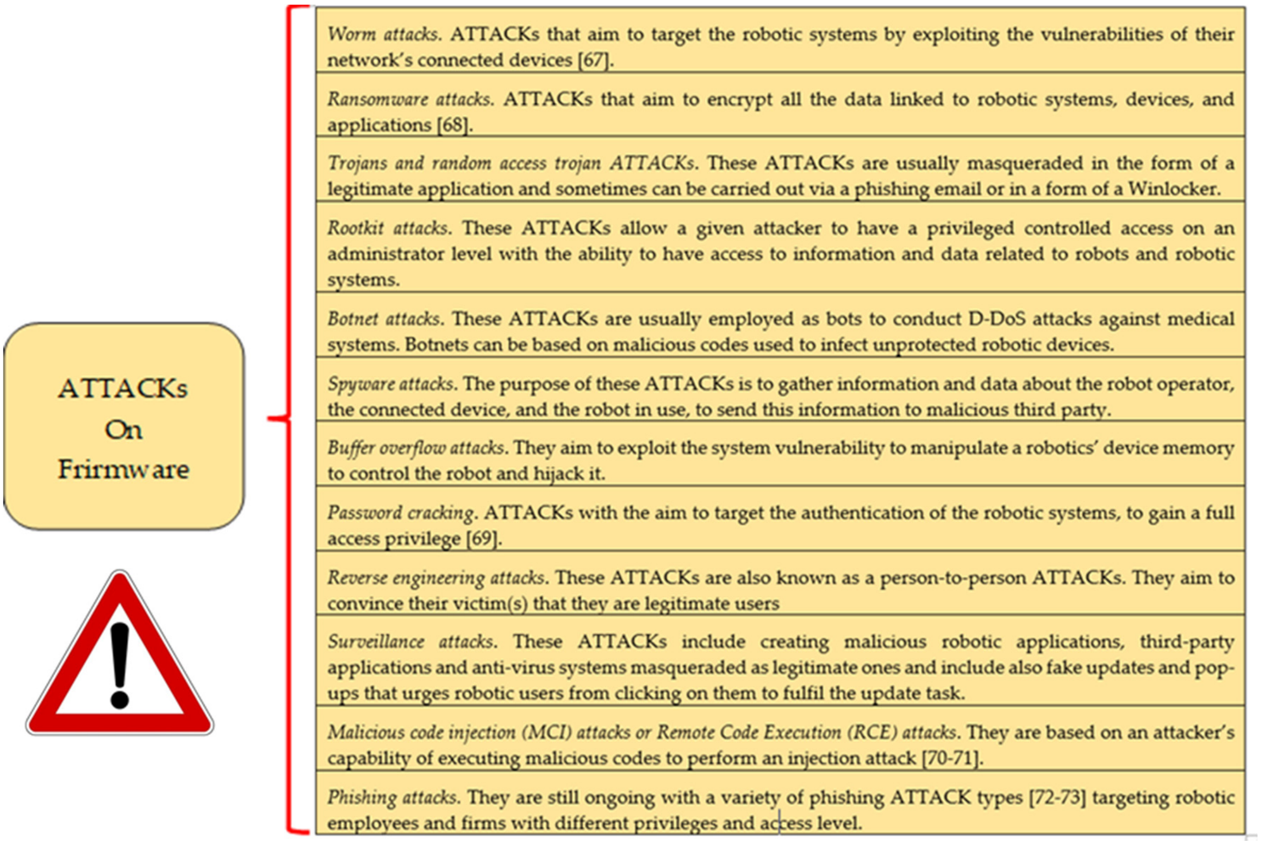
The Attacks can be arranged into three categories [21]: ATTACKs on the hardware, ATTACKs on firmware, ATTACKs on the communication. In the following, we summarize these categories in brief.

5.1. Attacks on the Hardware

These ATTACKs [21] vary from hardware Trojans up to phishing [63]. They allow the aggressor to create passages to gain unauthorized access up a full control [21,64]. In some cases, they can even have a full access to the hardware. We can also find the implementation ATTACKs or fault ATTACKs [64]. These are very dangerous and can cause to sensitive data damage or system corruption.

5.2. Attacks on the Firmware

According to [21,65,66], as the OS upgrading/maintenance is mainly performed using the internet, the OS is exposed to DoS and D-DoS ATTACKs, along with the indiscriminate programme execution, and root-kit ATTACKs. Furthermore, the Applications in the CRs, are vulnerable to application ATTACKs. These ATTACKs comprehend malware, worms, viruses, software Trojans ATTACKs, buffer overflow, and malicious code injection ATTACKs [67]. Figure 3 reports examples of these ATTACKs [21,67–73]:



Worm attacks. ATTACKs that aim to target the robotic systems by exploiting the vulnerabilities of their network's connected devices [67].

Ransomware attacks. ATTACKs that aim to encrypt all the data linked to robotic systems, devices, and applications [68].

Trojans and random access trojan ATTACKs. These ATTACKs are usually masqueraded in the form of a legitimate application and sometimes can be carried out via a phishing email or in a form of a Winlocker.

Rootkit attacks. These ATTACKs allow a given attacker to have a privileged controlled access on an administrator level with the ability to have access to information and data related to robots and robotic systems.

Botnet attacks. These ATTACKs are usually employed as bots to conduct D-DoS attacks against medical systems. Botnets can be based on malicious codes used to infect unprotected robotic devices.

Spyware attacks. The purpose of these ATTACKs is to gather information and data about the robot operator, the connected device, and the robot in use, to send this information to malicious third party.

Buffer overflow attacks. They aim to exploit the system vulnerability to manipulate a robotics' device memory to control the robot and hijack it.

Password cracking. ATTACKs with the aim to target the authentication of the robotic systems, to gain a full access privilege [69].

Reverse engineering attacks. These ATTACKs are also known as a person-to-person ATTACKs. They aim to convince their victim(s) that they are legitimate users

Surveillance attacks. These ATTACKs include creating malicious robotic applications, third-party applications and anti-virus systems masqueraded as legitimate ones and include also fake updates and pop-ups that urges robotic users from clicking on them to fulfil the update task.

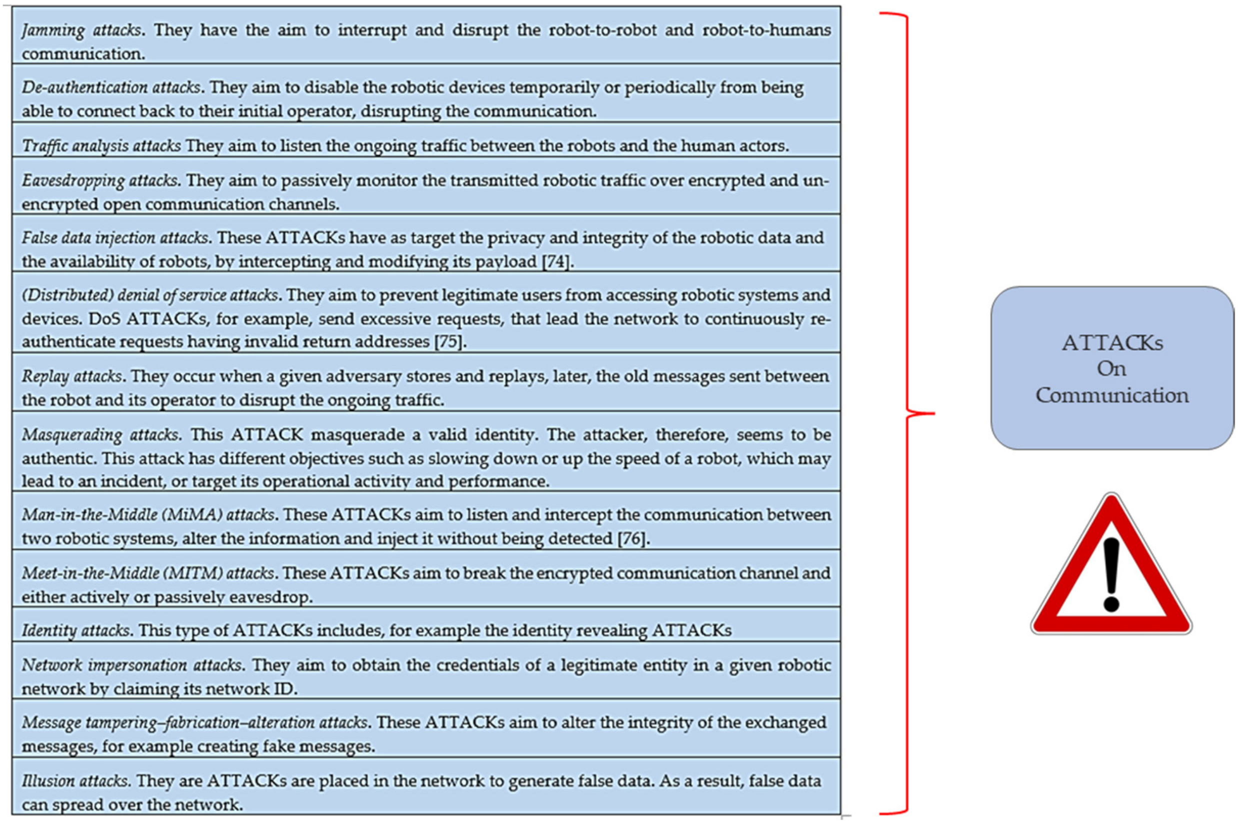
Malicious code injection (MCI) attacks or Remote Code Execution (RCE) attacks. They are based on an attacker's capability of executing malicious codes to perform an injection attack [70-71].

Phishing attacks. They are still ongoing with a variety of phishing ATTACK types [72-73] targeting robotic employees and firms with different privileges and access level.

Figure 3. Examples of ATTACKs on the firmware.

5.3. Attacks on Communications

Robotic communications are also exposed to different ATTACKs [21,74–77] that can affect different levels of security at different levels of communication (Figure 4):



Jamming attacks. They have the aim to interrupt and disrupt the robot-to-robot and robot-to-humans communication.

De-authentication attacks. They aim to disable the robotic devices temporarily or periodically from being able to connect back to their initial operator, disrupting the communication.

Traffic analysis attacks They aim to listen the ongoing traffic between the robots and the human actors.

Eavesdropping attacks. They aim to passively monitor the transmitted robotic traffic over encrypted and unencrypted open communication channels.

False data injection attacks. These ATTACKs have as target the privacy and integrity of the robotic data and the availability of robots, by intercepting and modifying its payload [74].

(Distributed) denial of service attacks. They aim to prevent legitimate users from accessing robotic systems and devices. DoS ATTACKs, for example, send excessive requests, that lead the network to continuously re-authenticate requests having invalid return addresses [75].

Replay attacks. They occur when a given adversary stores and replays, later, the old messages sent between the robot and its operator to disrupt the ongoing traffic.

Masquerading attacks. This ATTACK masquerade a valid identity. The attacker, therefore, seems to be authentic. This attack has different objectives such as slowing down or up the speed of a robot, which may lead to an incident, or target its operational activity and performance.

Man-in-the-Middle (MiMA) attacks. These ATTACKs aim to listen and intercept the communication between two robotic systems, alter the information and inject it without being detected [76].

Meet-in-the-Middle (MITM) attacks. These ATTACKs aim to break the encrypted communication channel and either actively or passively eavesdrop.

Identity attacks. This type of ATTACKs includes, for example the identity revealing ATTACKs

Network impersonation attacks. They aim to obtain the credentials of a legitimate entity in a given robotic network by claiming its network ID.

Message tampering–fabrication–alteration attacks. These ATTACKs aim to alter the integrity of the exchanged messages, for example creating fake messages.

Illusion attacks. They are ATTACKs are placed in the network to generate false data. As a result, false data can spread over the network.

Figure 4. Examples of ATTACKs on the communication.

6. Conclusions

6.1. Highlights

CRs [7] represent an opportunity for the health domain. The use of these robots has important implications. They can be used in surgery [7], in important and delicate clinical interventions both in presence and in tele-surgery. They can be used on frail patients, in rehabilitation processes [8]. They can be used in psychological and cognitive rehabilitation processes, as in the case of SRs, in children, elderly, and other subjects with disabilities [3,4]. Therefore, they have important physical and psychological implications during their use [9]. Furthermore, these devices, during their use, encounter important demographic-and-clinical data and other reserved information; all data that must be protected, in accordance with current regulations [1,2]. CS has consequently become a crucial issue. It concerns all the actors involved (from the design process to its use; from the manufacturer up to the patient and the caregiver). The study investigated the collocation of CRs in the context of CS studies in the health domain, also in comparison to other sectors. Problems and peculiarities were faced, investigating in different scientific database. They ranged from ethics and safety up to legislation and regulation issues.

The highlights of the study are as follows:

- A simple search on the Pubmed database, the most important database of the health domain, shows 12.785 results on the CS [12]. Among these, an important group [13] is dedicated to robotics. However, many studies on robotics linked to CS can be traced with the other keys safety and risk [14,15].
- CRs have peculiarities that make them unique. However, regarding some issues, the experience of robotics used in the IPCS robotics can be partly taken into consideration [16–20].

- CRs are complex mechatronic tools, but also HCI and devices integrated to eHealth [27,28,51]. Scientific support come also from both initiatives of scientific societies, operating in these sectors [27] and proper approaches on the insiders [28].
- Ethics has an important role and a peculiarity on CRs, such as on the SRs [29]. An in-depth analysis of the ethical issues in this discipline has identified two macro-sectors [30,31]. The first macro-sector is the ethics in a responsible research and innovation [30]. The second macro-sector is the ethics problem encountered while building moral CRs [31]. A strong connection emerges between ethical issues and CS from the examination of the two macro-sectors (also correlated). There is a strong need to rethink a CS connected to ethics issues.
- The models between the Cyber ATTACKs/ Software default/AI deficits and the physical/ psychological impact, have been identified [9]. They also embed the problems identified in the previous point [30,31]. These models show a wider range of CS problems than other consolidated MDs [57–62].
- Cyber ATTACKs applicable on the CRs, and the related impact, have been identified and categorized into three groups [21] concerning hardware [63,64], firmware [65–73], and communication [74–77].
- Targeted surveys with interviews and questionnaires regarding the CS behaviours of insiders with CRs will have to be conducted, as already been carried out, for example, in the health domain generally [28]. This will be useful for building medical knowledge.
- There are shadows in EU MD regulations [53]. First, it focuses a lot on manufacturers and little on recipients/ users. Second, [9] the compliance with CS requirements is challenging, in part due to the potential overlap of different certification schemes with varying geographical or product scope and evolution of external to the MDR regulations. Third, the intended use and certification, often, do not seem aligned.
- There are limits in the application of specific CS certifications. They are voluntary, as in the case of the Cybersecurity ACT [56].
- The CRs would need an ad hoc regulatory framework, in consideration of the peculiarities.

6.2. Reflections

We believe that, in the light of what is covered in our study, it is important to plan an acculturalization process on CS, with specific reference to CRs. This process must concern all the involved actors, from the builders up to the users, and the caregivers. It must be conducted in the different environments (e.g., home and the hospital). Training in this area must become an important issue. In addition, agreement initiatives (e.g., guidelines, consensus conferences, and technology assessment initiative [78–84]) considering CS could be welcome. Stakeholders will have to take actions in this area, through consensus initiatives (for example, considering the CS in consensus conferences), specific monitoring initiatives (for example through targeted surveys), and specific interventions on the training.

Author Contributions: Conceptualization, D.G.; methodology, D.G.; software, D.G., R.A.G.; validation, D.G., R.A.G.; formal analysis, D.G.; investigation, D.G.; resources, D.G., R.A.G.; data curation, D.G.; writing—original draft preparation, D.G.; writing—review and editing, All; visualization, All; supervision, All; project administration, D.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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.

References

1. Giansanti, D. Cybersecurity and the digital-health: The challenge of this millennium. *Healthcare* **2021**, *9*, 62. [CrossRef]
2. Giansanti, D.; Monoscalco, L. The cyber-risk in cardiology: Towards an investigation on the self-perception among the cardiologists. *Mhealth* **2021**, *7*, 28. [CrossRef]
3. Cobo Hurtado, L.; Viñas, P.F.; Zalama, E.; Gómez-GarcíaBermejo, J.; Delgado, J.M.; Vielba García, B. Development and usability validation of a social robot platform for physical and cognitive stimulation in elder care facilities. *Healthcare* **2021**, *9*, 1067. [CrossRef]
4. Sheridan, T.B. A review of recent research in social robotics. *Curr. Opin. Psychol.* **2020**, *36*, 7–12.
5. Mejia, C.; Kajikawa, Y. Bibliometric analysis of social robotics research: Identifying research trends and knowledgebase. *Appl. Sci.* **2017**, *7*, 1316.
6. Social Robots Market—Growth, Trends, COVID-19 Impact, and Forecasts (2021–2026). Available online: https://www.mordorintelligence.com/industry-reports/social-robots-market (accessed on 22 February 2021).
7. Dolic, Z.; Castro, R.; Moarcas, A. Robots in Healthcare: A Solution or a Problem? Study for the Committee on Environment, Public Health, and Food Safety. Luxembourg: Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament. 2019. Available online: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/638391/IPOL_IDA(2019)638391_EN.pdf (accessed on 25 November 2021).
8. Boldrini, P.; Bonaiuti, D.; Mazzoleni, S.; Posteraro, F. Rehabilitation assisted by robotic and electromechanical devices for people with neurological disabilities: Contributions for the preparation of a national conference in Italy. *Eur. J. Phys. Rehabil. Med.* **2021**, *57*, 458–459. [CrossRef]
9. Fosch-Villaronga, E.; Mahler, T. Safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Comput. Law Secur. Rev.* **2021**, *41*, 105528.
10. European Foresight Monitoring Network, EFMN (2008) Roadmap Robotics for Healthcare. Foresight Brief No. 157. Available online: http://www.foresight-platform.eu/wp-content/uploads/2011/02/EFMN-Brief-No.-157_Robotics-for-Healthcare.pdf (accessed on 22 February 2021).
11. European Parliament Resolution of 12 February 2019 on a Comprehensive European Industrial Policy on Artificial Intelligence and Robotics (2018/2088(INI)). Available online: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.pdf (accessed on 22 February 2021).
12. Specific Research on the Pubmed Database. Available online: https://pubmed.ncbi.nlm.nih.gov/?term=%28cybersecurity%29+AND+%28healthcare%29&sort=date&size=200 (accessed on 25 November 2021).
13. Specific Research on the Pubmed Database: (cybersecurity) AND (healthcare) AND (care robots). Available online: https://pubmed.ncbi.nlm.nih.gov/?term=%28cybersecurity%29+AND+%28healthcare%29+AND+%28care+robots%29&sort=date&size=200 (accessed on 25 November 2021).
14. Specific Research on the Pubmed Database: (safey[Title/Abstract]) AND (robot). Available online: https://pubmed.ncbi.nlm.nih.gov/?term=%28safey%5BTitle%2FAbstract%5D%29+AND+%28robot%29&sort=date (accessed on 25 November 2021).
15. Specific Research on the Pubmed Database: (risk [Title/Abstract]) AND (robot). Available online: https://pubmed.ncbi.nlm.nih.gov/?term=%28risk+%5BTitle%2FAbstract%5D%29+AND+%28robot%29&sort=date&size=200 (accessed on 22 November 2021).
16. Murashov, V.; Hearl, F.; Howard, J. Working safely with robot workers: Recommendations for the new workplace. *J. Occup. Environ. Hyg.* **2016**, *13*, D61–D71. [CrossRef]
17. Missala, T. Paradigms and safety requirements for a new generation of workplace equipment. *Int. J. Occup. Saf. Ergon.* **2014**, *20*, 249–256. [CrossRef] [PubMed]
18. Bortot, D.; Ding, H.; Antonopolous, A.; Bengler, K. Human motion behavior while interacting with an industrial robot. *Work* **2012**, *41* (Suppl. 1), 1699–1707. [CrossRef]
19. Guangnan, Z.; Tao, H.; Rahman, M.A.; Yao, L.; Al-Saffar, A.; Meng, Q.; Liu, W.; Yaseen, Z.M. Security and privacy issues related to the workplace-based security robot system. *Work* **2021**, *68*, 871–879. [CrossRef]
20. Zheyuan, C.; Rahman, M.A.; Tao, H.; Liu, Y.; Pengxuan, D.; Yaseen, Z.M. Need for developing a security robot-based risk management for emerging practices in the workplace using the Advanced Human-Robot Co. *Work* **2021**, *68*, 1–10.
21. Yaacoub, J.A.; Noura, H.N.; Salman, O.; Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **2021**, *19*, 1–44. [CrossRef]
22. Vulpe, A.; Crăciunescu, R.; Drăgulinescu, A.M.; Kyriazakos, S.; Paikan, A.; Ziafati, P. Enabling security services in socially assistive robot scenarios for healthcare applications. *Sensors* **2021**, *21*, 6912. [CrossRef]
23. Liu, Y.; Yi, Y.; Deng, P.; Zhang, W. Preclinical evaluation of the new EDGE SP 1000 single-port robotic surgical system in gynecology minimal access surgery. *Surg. Endosc.* **2021**, 1–6, (Online ahead of print). [CrossRef]
24. Li, I.H.; Lin, Y.S.; Lee, L.W.; Lin, W.T. Design, manufacturing, and control of a pneumatic-driven passive robotic gait training system for muscle-weakness in a lower limb. *Sensors* **2021**, *21*, 6709. [CrossRef]
25. Lhotska, L. Application of industry 4.0 concept to health care. *Stud. Health Technol. Inform.* **2020**, *273*, 23–37. [CrossRef] [PubMed]
26. Jarota, M. Artificial intelligence and robotisation in the EU—should we change OHS law? *J. Occup. Med. Toxicol.* **2021**, *16*, 18. [CrossRef]
27. HCI 2020 International 22st International Conference on Human—Computer Interaction. Available online: https://2020.hci.international/files/HCII2020_Final_Program.pdf (accessed on 25 November 2021).

28. Coventry, L.; Branley-Bell, D.; Sillence, E.; Magalini, S.; Mari, P.; Magkanaraki, A.; Anastasopoulou, K. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In Proceedings of the 22nd International Conference on Human Computer Interaction, Copenhagen, Denmark, 19–24 July 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 105–122.
29. Specific Research on the Pubmed Database: (social robot) AND (ethics). Available online: https://pubmed.ncbi.nlm.nih.gov/?term=%28social+robot%29+AND+%28ethics%29&sort=date&size=200 (accessed on 25 November 2021).
30. Stahl, B.C.; Coeckelbergh, M. Ethics of healthcare robotics: Towards responsible research and innovation. *Robot. Auton. Syst.* **2016**, *86*, 152–161.
31. Gordon, J.S. Building moral robots: Ethical pitfalls and challenges. *Sci. Eng. Ethics* **2020**, *26*, 141–157. [CrossRef]
32. Coeckelbergh, M. Human development or human enhancement? A methodological reflection on capabilities and the evaluation of information technologies. *Ethics Inf. Technol.* **2011**, *13*, 81–92. [CrossRef]
33. Coeckelbergh, M. Are emotional robots deceptive? *IEEE Trans. Affect. Comput.* **2012**, *3*, 388–393. [CrossRef]
34. Coeckelbergh, M. E-care as craftsmanship: Virtuous work, skilled engagement, and information technology in health care. *Med. Health Care Philos.* **2013**, *16*, 807–816.
35. Coeckelbergh, M. Good healthcare is in the "how": The quality of care, the role of machines, and the need for new skills. In *Machine Medical Ethics*; van Rysewyk, S.P., Pontier, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 33–48.
36. Decker, M.; Fleischer, T. Contacting the brain—aspects of a technology assessment of neural implants. *Biotechnol. J.* **2008**, *3*, 1502–1510. [CrossRef]
37. Sharkey, A.; Sharkey, N. Granny and the robots: Ethical issues in robot care for the elderly. *Ethics Inform. Technol.* **2010**, *14*, 27–40.
38. Sparrow, R.; Sparrow, L. In the hands of machines? The future of aged care. *Minds Mach.* **2006**, *16*, 141–161.
39. Whitby, B. Do you want a robot lover. In *Robot Ethics: The Ethical and Social Implications of Robotics*; Lin, P., Abney, K., Bekey, G.A., Eds.; MIT Press: Cambridge, MA, USA, 2011; pp. 233–249.
40. Anderson, S.L.; Anderson, M. *Towards a principle-based healthcare agent, In Machine Medical Ethics*; van Rysewyk, S.P., Pontier, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 67–78.
41. Coeckelbergh, M. Artificial agents, good care, and modernity. *Theor. Med. Bioeth.* **2015**, *36*, 265–277.
42. Tonkens, R. Ethics of robotic assisted dying. In *Machine Medical Ethics*; van Rysewyk, S.P., Pontier, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 207–232.
43. van Rysewyk, S.P.; Pontier, M. A hybrid bottom-up and top-down approach to machine medical ethics: Theory and data. In *Machine Medical Ethics*; Van Rysewyk, S.P., Pontier, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 93–110.
44. Whitby, B. Automating medicine the ethical way. In *Machine Medical Ethics*; van Rysewyk, S.P., Pontier, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; p. 233.
45. Moor, J.H. The nature, importance, and difficulty of machine ethics. *Res. Gate* **2006**, *21*, 18–21.
46. Robot ethics: The ethical and social implications of robotics. In *Intelligent Robotics and Autonomous Agents*; Lin, P.; Abney, K.; Bekey, G.A. (Eds.) MIT Press: Cambridge, MA, USA, 2014.
47. Wallach, W.; Allen, C. *Moral Machines: Teaching Robots Right from Wrong*; Oxford University Press: Oxford, UK, 2010.
48. Anderson, M.; Anderson, S.L. *Machine Ethics*; Cambridge University Press: Cambridge, MA, USA, 2011.
49. Gunkel, D.J.; Bryson, J. The machine as moral agent and patient. *Philos. Technol.* **2014**, *27*, 5–142.
50. Anderson, S.L. Machine metaethics. In *Machine Ethics*; Anderson, M., Anderson, S.L., Eds.; Cambridge University Press: Cambridge, MA, USA, 2011; pp. 21–27.
51. Finocchiaro, G. Protection of privacy and cyber risk in healthcare. *Pharm. Policy Law.* **2018**, *19*, 121–123.
52. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety 2001. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52003PC0048 (accessed on 25 November 2021).
53. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC.2017. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0745&from=IT (accessed on 25 November 2021).
54. NIS Directive (The Directive on Security of Network and Information Systems). Available online: https://www.itgovernance.eu/fi-fi/nis-directive-fi (accessed on 25 November 2021).
55. Complete Guide to GDPR Compliance. Available online: https://gdpr.eu/ (accessed on 25 November 2021).
56. Shaping Europe's Digital Future. Available online: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act (accessed on 25 November 2021).
57. Fraiche, A.M.; Matlock, D.D.; Gabriel, W.; Rapley, F.A.; Kramer, D.B. Patient and provider perspectives on remote monitoring of pacemakers and implantable cardioverter-defibrillators. *Am. J. Cardiol.* **2021**, *149*, 42–46. [CrossRef]
58. Tomaiko, E.; Zawaneh, M.S. Cybersecurity threats to cardiac implantable devices:room for improvement. *Curr. Opin. Cardiol.* **2021**, *36*, 1–4. [CrossRef]
59. Saxon, L.A.; Varma, N.; Epstein, L.M.; Ganz, L.I.; Epstein, A.E. Rates of adoption and outcomes after firmware updates for food and drug administration cybersecurity safety advisories. *Circ. Arrhythm. Electrophysiol.* **2020**, *13*, e008364. [CrossRef]
60. Burnside, M.; Crocket, H.; Mayo, M.; Pickering, J.; Tappe, A.; de Bock, M. Do-it-yourself automated insulin delivery: A leading example of the democratization of medicine. *J. Diabetes Sci. Technol.* **2020**, *14*, 878–882. [CrossRef]

61. Woldaregay, A.Z.; Årsand, E.; Walderhaug, S.; Albers, D.; Mamykina, L.; Botsis, T.; Hartvigsen, G. Data-driven modeling and prediction of blood glucose dynamics:Machine learning applications in type 1 diabetes. *Artif. Intell. Med.* **2019**, *98*, 109–134. [CrossRef]
62. DeBoer, M.D.; Breton, M.D.; Wakeman, C.; Schertz, E.M.; Emory, E.G.; Robic, J.L.; Kollar, L.L.; Kovatchev, B.P.; Cherñavvsky, D.R. Performance of an artificial pancreas system for young children with type 1 diabetes. *Diabetes Technol. Ther.* **2017**, *19*, 293–298. [CrossRef]
63. Gaikwad, N.B.; Ugale, H.; Keskar, A.; Shivaprakash, N.C. The internet of battlefield things (IoBT) based enemy localization using soldiers location and gunshot direction. *IEEE Internet Things J.* **2020**, *7*, 11725–11734.
64. Tehranipoor, M.; Koushanfar, F. A survey of hardware Trojan taxonomy and detection. *IEEE Des. Test Comput* **2010**, *27*, 10–25.
65. Wang, X.; Mal-Sarkar, T.; Krishna, A.; Narasimhan, S.; Bhunia, S. Software exploitable hardware Trojans in embedded processor. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*; IEEE: Piscataway Township, NJ, USA, 2012; pp. 55–58.
66. Elmiligi, H.; Gebali, F.; El-Kharashi, M.W. Multi-dimensional analysis of embedded systems security. *Microprocess. Microsyst.* **2016**, *41*, 29–36.
67. Clark, G.W.; Doran, M.V.; Andel, T.R. Cybersecurity issues in robotics. In *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*; IEEE: Piscataway Township, NJ, USA, 2017; pp. 1–5.
68. Falliere, N.; Murchu, L.O.; Chien, E. W32. stuxnet dossier.White paper, Symantec Corp. *Secur. Response* **2011**, *5*, 29.
69. Fruhlinger, J. What is Wannacry Ransomware, How does It Infect, and Who Was Responsible. 2017. Available online: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (accessed on 25 November 2021).
70. Bellovin, S.M.; Merritt, M. Encrypted key exchange: Password based protocols secure against dictionary attacks. In *1992 IEEE Computer Society Symposium on Research in Security and Privacy*; IEEE: Piscataway Township, NJ, USA, 1992; pp. 72–84.
71. Kc, G.S.; Keromytis, A.D.; Prevelakis, V. Countering code injection attacks with instruction-set randomization. In Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, 27–30 October 2003; pp. 272–280.
72. Miller, J.; Williams, A.B.; Perouli, D. A case study on the cybersecurity of social robots. In Proceedings of the Companion of the 2018 ACM/IEEE International Conference on Human–Robot Interaction, Chicago, IL, USA, 5–8 March 2018; pp. 195–196.
73. Shahbaznezhad, H.; Kolini, F.; Rashidirad, M. Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *J. Comput. Inf. Syst.* **2020**, *61*, 1–12.
74. Alabdan, R. Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet* **2020**, *12*, 168.
75. Mo, Y.; Garone, E.; Casavola, A.; Sinopoli, B. False data injection attacks against state estimation in wireless sensor networks. In *2010 49th IEEE Conference on Decision and Control (CDC)*; IEEE: Piscataway Township, NJ, USA, 2010; pp. 5967–5972.
76. Senie, D.; Ferguson, P. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. *Network* **1998**.
77. Navas, R.E.; Le Bouder, H.; Cuppens, N.; Cuppens, F.; Papadopoulos, G.Z. Do not trust your neighbors! A small IoT platform illustrating a man-in-the-middle attack. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, St. Malo, France, 5–7 September 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 120–125.
78. Evidence-Based Medicine Guidelines. Available online: https://www.ebm-guidelines.com/dtk/ebmg/home (accessed on 25 November 2021).
79. Luce, B.R.; Drummond, M.; Jönsson, B.; Neumann, P.J.; Schwartz, J.S.; Siebert, U.; Sullivan, S.D. EBM, HTA, and CER: Clearing the confusion. *Milbank Q.* **2010**, *88*, 256–276. [CrossRef]
80. Office of Technology Assessment. 1978. Assessing the Efficacy and Safety of Medical Technologies. September. NTIS order #PB-286929. Available online: http://www.fas.org/ota/reports/7805.pdf (accessed on 25 November 2009).
81. INAHTA (International Network of Agencies for Health Technology Assessment). HTA Resources. 2009. Available online: http://www.inahta.org/HTA/ (accessed on 25 November 2009).
82. Candiani, G.; Colombo, C.; Daghini, R.; Magrini, N. Come Organizzare una Conferenza di Consenso. Manuale Metodologico, Roma, ISS-SNLG. 2009. Available online: https://www.psy.it/wp-content/uploads/2018/02/Manuale-Metodologico-Consensus.pdf (accessed on 25 November 2021).
83. Arcelloni, M.C.; Milani, C. Consensus Conference: Uno Strumento per la Pratica Clinica Riferimenti Storico-Metodologici e Stato Dell'arte dei Lavori Italiani sul Disturbo Primario del Linguaggio e sui Disturbi Specifici dell'Apprendimento. Available online: https://rivistedigitali.erickson.it/il-tnpee/archivio/vol-1-n-1/riferimenti-storico-metodologici-e-stato-dellarte-dei-lavori-italiani-sul-disturbo-primario-del-linguaggio-e-sui-disturbi-specifici-dellapprendimento/ (accessed on 25 November 2021).
84. McGlynn, E.A.; Kosecoff, J.; Brook, R.H. Format and conduct of consensus development conferences. Multi-nation comparison. *Int. J. Technol. Assess Health Care* **1990**, *6*, 450–469. [CrossRef]