Exploring Care Robots' Cybersecurity Threats From Care Robotics Specialists' Point of View

Jyri Rajamäk and Marina Järvinen
Laurea University of Applied Sciences, Espoo, Finland
jyri.rajamaki@laurea.fi
marina.jarvinen@student.laurea.fi

Abstract: Care robots can perform tasks related to physical or mental care; assisting in daily tasks or rehabilitation, independently or semi-automatically. Care robots are exploitable in home-care, nursing homes, or other care facilities. Care robots have the potential to solve several challenges related to aging people. However, care robots suffer have similar cybersecurity problems as other information and communication technology (ICT) devices. In addition, the cybersecurity threats of care robots have been studied less than those of industrial robots. This study's purpose is to map cybersecurity threats related to care robots from the perspective of care robotics specialists. The study consists of thematic interviews of six purposive-selected specialists in care robotics. A semi-structured thematic interview guide based on the literature view of previous studies, facilitates the conversations at the interviews. All interviews were transcribed verbatim, analyzed by deductive content analysis, and the remaining material was analyzed by inductive content analysis. According to the interviewed specialists, care robots' cybersecurity threats are associated with the same risks and threats as the use of other ICT devices or robots. Most potential threats are considered to be remote access of care robots, spying, and eavesdropping. Network connectivity is seen as the main interface to the realization of cybersecurity threats in care robotics. New features such as artificial intelligence and machine learning are considered to create more opportunities for new threats. Experts also highlight the underlying human factors behind cybercrime. According to the results, more studies exploring the motives for cybercrime against care robots and the potential benefits derived from it are needed to determine the likelihood of the realization of threats to care robots are needed. Cybersecurity is a race against cybercrime and finding a balance between significant and acceptable risks. In the future, a service ecosystem should be developed which guarantees the safety of care robots throughout their life-cycle: during the design and development phase, deployment and user guidance, maintenance, and reuse of the robot. Additionally, it is important to take into account how new robust operating models can withstand failures and how critical services can be secured in the event of a cybersecurity threat.

Keywords: care robot, cybersecurity of robots, cybercrime, thematic interviews, hijacking, rehabilitation systems

1. Introduction

As the population ages, care for the elderly will face new challenges as the demand for care increases. Care robots are cyber-physical systems that can perform tasks related to physical or mental care. They can be used to care for a person at home, in a care home, or in a care facility. They can also facilitate the work and co-operation of carers between home and care, for example through remote connections (Van Aerschot & Parviainen, 2020; Särkikoski, Turja & Parviainen, 2020).

Robots can make everyday life easier, create a sense of security, and perform a variety of tasks, but as a misfortune, they suffer from similar cybersecurity issues that computers have suffered from for a decade (Lera, Llamas, Guerrero & Olivera, 2017). Cybersecurity threats related to service and care robots have been studied much less than, for example, the cybersecurity of robots intended for industrial environments (Lera et al. 2017; Fosch-Villaronga & Mahler, 2021).

This qualitative study highlights the current view of care robotics experts on the cybersecurity of care robots and the real cybersecurity threats associated with their use. The research question is, "What are the cybersecurity threats to care robots?" The goal of threat mapping is to increase awareness, making it easier for both service providers and end-users to critically assess the threats associated with the use of devices and the risks they are prepared to take.

2. Literature review

A 'robot' refers to a reprogrammable mechatronic device that influences its environment by means of sensors and actuators (Särkikoski et al., 2020). Typically, robots are divided into industrial and service robots depending on whether they are used for the benefit of industry or perform tasks useful to humans (Fosch-Villaronga & Mahler, 2021). Robots are directly involved in human life and raise crucial ethical problems for our society (Tzafestas, 2018). Table 1 presents examples of healthcare robot applications according to the Policy Department for Economic, Scientific and Quality of Life Policies of the European Parliament.

Table 1: Examples of healthcare robot (Dolic, Castro & Moarcas, 2019).

Healthcare robot applications	
Robotic surgery	Allowing more accurate, less invasive and remote interventions relying on the availability and assessment of vast amounts of data
Care and socially assistive robots	Allowing to meet the expanding demands for long-term care from an aging population affected by multi-morbidities
Rehabilitation systems	Supporting the recovery of patients as well as their long-term treatment at home rather than at a healthcare facility
Training for health and care workers	Offering support for continuous training and life-long learning initiatives

Several articles talk about service robots, social robots, and care robots in the same context. A 'service robot' is a robot that is able to perform partially or completely independently services that are beneficial to human well-being or the environment. A 'social robot' complements, increases, or replaces human social interaction (Särkikoski et al. 2020). 'Care robots' can perform tasks related to physical or mental care independently or semi-automatically, such as assisting in daily tasks, rehabilitation, or mental care (Van Aerschot & Parviainen, 2020; Särkikoski et al. 2020).

Robots can often be programmed to be modified for different uses, so it may not be completely unambiguous to determine whether a robot is a care robot based on a purpose other than the use or environment (Fosch-Villaronga & Mahler, 2021). Thus, if the robot is used, for example, to care for children, the elderly and the disabled, it is a care robot, even if the same robot could be programmed elsewhere to deliver, for example, the work of a lobby clerk. A social robot can also be a care robot if its purpose is related to mental care.

Care robots can help with daily activities, provide companionship and a sense of security. Efforts are being made to develop and bring robots to the market, and care robots have been tested in Finland, e.g. in the care of the elderly (Schönberg, 2017) and the care of people with memory problems (Forum Virium, 2020). So far, however, it has not been possible to develop a care robot that could completely replace human work in helping the elderly in their daily activities. Monitoring devices, automated drug dispensers, robotic pets, cell phone attendance devices, and hospital logistics are already in use, but they are only capable of simple spoken language interactions or modest repetitive tasks, not situationally demanding day-to-day operations (Van Aerschot & Parviainen, 2020).

Robots can identify, process, and store the world around them, and they are constantly collecting data. Robots suffer from similar cybersecurity issues that computers have suffered from for a decade (Lera et al., 2017). Robot operation (such as navigation, speech, object recognition, etc.) requires heavy computing enabled by cloud services. As the number of interconnected systems and devices increases, so does the potential for vulnerabilities in the systems and the risk of malicious attacks (Fosch-Villaronga & Mahler, 2021).

3. Research method

This qualitative study explores the views of care robot experts (researcher, developer, or service provider) on what cybersecurity threats pose to care robots by thematic interviews lasting 35 to 75 minutes, carried out in the fall of 2021. The body of the interview questions was created based on literature. The themes were:

- cybersecurity of care robots at the present,
- potential cybersecurity threats to care robots, and
- the biggest risks to the cybersecurity of care robots.

With six interviews, saturation was observed. The accumulated material was analyzed with a theory-based analysis, in which the themes of the interviews also served as categories to which the material was related. The results of the interviews were also compared with the literature. The remaining material after the theory-based analysis was also analyzed by material-based content analysis to reveal the main aspects of the material that did not fit into the analysis framework described above.

4. Results

Figure 1 summarizes the results of the interviews. Experts' views on cybersecurity in care robotics fall into the three theoretical categories outlined above. In addition, the 'cybercrime' perspective emerged in the evidence-based analysis.

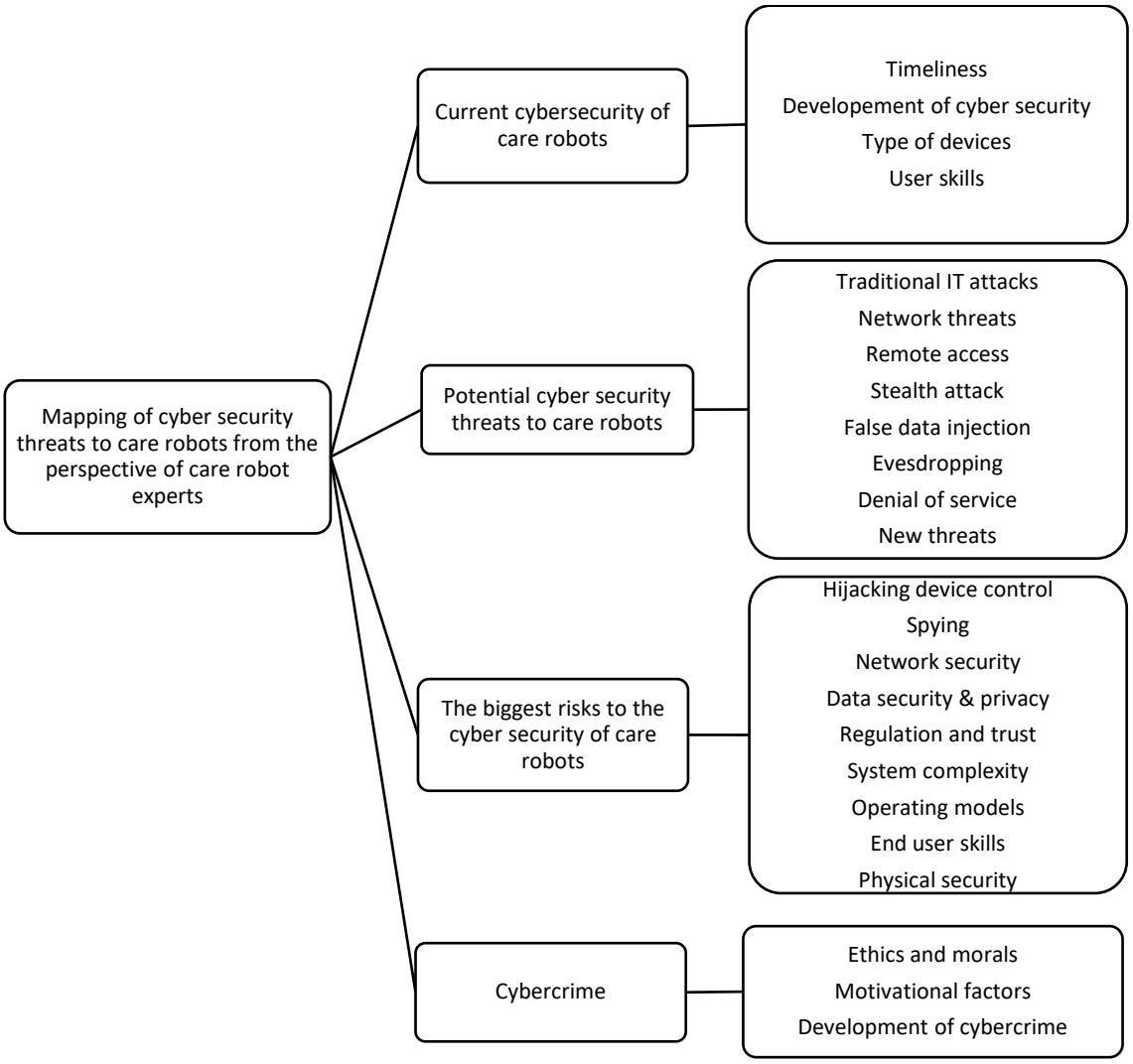

Figure 1: Care robot experts' views on the cybersecurity of care robots

4.1 Current cybersecurity of care robots

4.1.1 Timeliness

The interviewed experts are not worried about the cybersecurity of care robots at the present because there are few care robots in use or available on the market. The experts have not heard of the threats to care robots and feel that there is little talk about the subject. On the other hand, the experts view that the cybersecurity of care robots is a topical issue, as the use of care robots, like all other devices, involves risks, and as the number of care robots increases, so does the interest of cybercriminals in care robots. At present, however, it was felt more likely that cybercrime would target other devices that are already in wide use.

The views of interviewed experts on the use of the devices currently support previous studies. For example, Van Aerschot and Parviainen (2020) have found that care robots are hardly in use yet, although care robots are a possible solution to the future shortage of nurses and home carers as the population ages.

4.1.2 Development of cybersecurity

According to the interviewed experts, the development of functionality is currently a priority in the design and development of care robots, and thus the cybersecurity aspects of care robots are receiving less attention. The experts point out that cybersecurity focuses on data-related threats and security and does not take into account the threats that the care robot may pose to the physical environment.

Care robots are cyber-physical systems that combine hardware and software components, network and communication processes, mechanical actuators, controllers, operating systems, and sensors to interact with the physical world (Quarta et al., 2017). The view that robot's cybersecurity issues focus more on data-related threats than on physical-related threats has not been presented in previous studies. In general, however, the view of the experts is in line with Fosch-Villaronga and Mahler (2021) that the development of care robotics focuses more on the development of functionality than safety. Investing in data security is understandable because a lot of personal data is processed in social and health care, as well as sensitive data related to customers, which is why confidentiality, privacy, data integrity, and accessibility are key (Vuorinen, 2019). However, threats to physical security need to be increasingly addressed so that they do not become a problem in the future as the physical characteristics of care robots develop.

4.1.3 Type of devices

Currently, the term 'care and socially assistive robotics' includes certain types of medical, wellness technology, and other devices. This is problematic for equipment development. Telepresence and remote access robots are available for homes and home environments, but the experts have no information on where or how much these robots are used. Experts believe the security of remote access robots is at the same level as that of typical remote connections, i.e. they include base-level protection, and are vulnerable to cybersecurity threats. The safety of non-medical devices was uncertain, according to experts.

Experts consider the implementation of cybersecurity for medical devices to be mandatory, as the regulation of medical devices requires that the security of the devices be taken care of. In Finland, medical devices are under the control of the National Supervisory Authority for Welfare and Health (Valvira). Experts believe that there is no guarantee that the cybersecurity of a device will be ensured if it is not classified as a medical device because there is no control over welfare technology.

The literature also highlights the problematic nature of legislation on care robots (Holder et al., 2016; Fosch-Villaronga and Golia, 2019a; Fosch-Villaronga and Golia, 2019b). It is unclear how care robots can be legally classified because classification depends on their intended use, so these robots could be seen as either medical devices or general products, which are regulated differently (Fosch-Villaronga and Mahler 2021).

4.1.4 User skills

According to the interviewed experts, user skills affect the implementation of cybersecurity in care robots in two ways; when purchasing the device and when using the device. If a device does not have a rating for a medical device, the end-user is practically unable to deduce the level of security of the device to be acquired. User skills also affect the safety of equipment during use: it is difficult to make robots safe if they are not used following the principles designed by the manufacturer.

Clear communication about the level of cybersecurity of care robots is most important to the implementation of cybersecurity, as it is unclear whether robot vendors can assess the level of robot security (Fosch-Villarongan & Mahler, 2021; Lera et al. 2017). The experts emphasize the importance of clear communication from the perspectives of the service provider and end-user. The knowledge and understanding of these parties may not be sufficient to enable them to make informed decisions and risk assessments regarding the use of the equipment.

4.2 Potential cybersecurity threats to care robots

Care robots differ technically very little from other information and communication technology ICT equipment already in use making the attacks and the methods used on them technically the same as on other devices. So, care robots are subject to the same risks as other ICT devices. According to experts, traditional, purely computer-based information security attacks are also possible on care robots; the methods for implementing the attacks are the same as for other ICT devices. Interviews show that care robots are exposed to virtually all traditional security threats as well as threats related to the physical nature of robots. The possible threats perceived by experts are therefore in line with the literature (c.f. Lera et al.,2017; Rousku, 2014). The following is a more detailed discussion of potential cybersecurity threats that come up from interviews.

4.2.1 Remote access and network threats

Controlling the robot remotely brings with it threats. For example, hijacking device control with remote access is one of the potential cyber threats to care robots. Although all experts interviewed say hijacking is a potential threat, opinions are divided on whether the threat is likely or not.

Network connections expose care robots to a variety of threats, and experts feel that networks play a key role in how secure different devices are. The need for a network connection depends on the purpose and characteristics of the care robots, and the more complex and interactive devices are developed, the more important the network connection will be. Experts see that all of the above threats are more likely to occur if the device is connected to the Internet. The view of the interviewed experts is in line with the literature (c.f. Lera et al., 2017; Rousku, 2014) that all robots connected to the network can be a risk to their users because an outsider can access the devices via the network.

4.2.2 Stealth attack

A stealth attack, i.e., an attack in which an attacker gets to manipulate the operation of the robot's sensors and thus, for example, cause a robot to collide, is also a potential threat. Some of the interviewees think that since similar attacks are possible on other mobile robots, they can also be targeted at care robots, especially if the robot is poorly protected. Other experts find it difficult to find the motivation to carry out such attacks.

4.2.3 False data injection

Attacks in which the data processed by the robot can be modified are possible and, in certain situations, even easy to implement. Experts agree that the consequences of such a threat may be critical, but opinions differ on whether the threat is likely.

4.2.4 Eavesdropping

Eavesdropping and watching in secret are the most prominent issues that arise from the interviews. They are potential and probable threats because similar attacks have been carried out on other robots with microphones and cameras. According to experts, it is likely that particularly vulnerable remote access robots could be used for espionage, as their level of security may not be enough at present.

4.2.5 Denial-of-service

Two perspectives on denial-of-service attacks exist: care robots can be used to implement denial-of-service attacks, and denial-of-service attacks can be used to block the service provided by the robot. Experts see denial-of-service attacks as potential threats from both perspectives. On the other hand, devices that are not connected to the Internet are safe from the point of view of the denial of service. Experts believe that if the device is not connected to the Internet, for example, blocking remote connections will have little effect on the operation of the device. Also, offline devices cannot be used to carry out denial-of-service attacks.

4.2.6 New threats

The constant development of care robotics also brings new threats that have not been identified in previous studies. In this study, experts highlighted that the integration of new technologies, such as the use of cloud services, artificial intelligence, and machine learning in care robotics, creates opportunities for new attacks. In addition, unlike previous studies, experts stressed that in the future, physical risks will become more central to cybersecurity as the physical properties of care robots are developed.

4.3 The biggest cybersecurity risks of care robots

4.3.1 Hijacking device control and spying

Experts see that one of the biggest threats to cybersecurity for care robots is the hijacking of device control. Through the hijacking of a care robot, a cybercriminal can do practically all the same things that a user could do with the device, for example, access device information and spy on device users. In the case of a physically mobile device, an attacker can also cause physical damage to the robot environment, or even to the end-user of the robot, through the hijacking of the device.

Experts say another vast threat is spying. Using a care robot to eavesdrop on and/or watch in secret is easy to implement and possible to implement for a wide range of people. According to experts, the benefit-to-input ratio obtained by criminals is greatest through spying.

4.3.2 Network

Experts think network security, especially remote connections, is one of the most significant risks in the cybersecurity of care robots. The network connection is often the interface that allows the safety and security of care robots to be compromised. Isolated local area networks are slightly more secure than remote internet access, but experts see that it is also possible to access them on the spot. According to experts, the security of current remote applications is at a basic level, which makes them possible targets of hacking.

4.3.3 Data security and privacy

Experts are concerned about the security of the data collected by care robots. In particular, data protection issues arise when personal data is stored in cloud services. The concern is how to be able to secure and be sure that the data is recovered, stored, and disposed of correctly and that the data is not accessed by the wrong parties. Experts also raise concerns about maintaining data integrity.

4.3.4 Regulation and trust

In previous studies, the cybersecurity of care robots has often been addressed from a fairly technical perspective. However, all the risks associated with care robotics are not limited to the care robots themselves and their use. The current lack of legislation on cybersecurity underlines the trustfulness of the manufacturer and supplier of the care robot. Experts representing the service provider's point of view think that at the moment, you have to trust that the manufacturer of the care robot has taken safety and security considerations into account and has made the devices as safe and secure as possible. A risk factor for non-medical devices is that the only guarantee for the safety and security of the devices is the supplier's promise.

4.3.5 System complexity & operating models

Care robots may be part of a large system with a complex operating model. In this case, the interference may be to some other part of the system, which will cause the care robots to malfunction. According to experts, changes in operating models are risk factors. When the implementation of operations is designed with the help of robots, the damage can be vast if, for some reason, the robots do not work. Returning to the old operating model can be difficult and time-consuming. From the end-user's point of view, the malfunctions of the care robot can be very critical, depending on the criticality of the tasks performed by the care robots. Experts also see the risk that systems and service robots are subject to vulnerabilities in both the upgrade and operating systems throughout their lifecycle.

This is in line with Fosch-Villaronga & Mahler (2021); as the number of interconnected systems and devices increases, so do the cyber risks.

4.3.6 End-user

According to experts, end-users of care robots are associated with risk factors from a safety and security point of view. Experts are not convinced that end-users will necessarily take care of the security of their own homes and networks. Experts are also not convinced that end-users will act following data security principles.

Experts representing the development and manufacturing of care robots point out that it is difficult to make the equipment safe if it is not used following the principles designed by the manufacturer. The view is in line with previous studies (Lera et al., 2017; Fosch-Villarongan & Mahler, 2021). Vuorinen (2019) also states that e.g. rigid software can entice users of devices to circumvent information security mechanisms, which may result in users not changing their default passwords or using the same user ID. In other words, the user's competence is also central to the realization of the cybersecurity of the devices in use. When the end-users of care robotics are the elderly, concerns arise about their potentially deficient digital skills. Also, human memory and other characteristics do not usually improve with aging. According to experts, it is likely that as a person ages, he or she may no longer remember or know how to use the device and take care of data security.

4.3.7 Physical security

Experts see that the risks associated with the physique of robots will increase as the physical properties of the robots, such as the ability to manipulate objects, improve. In addition, experts think that if a cybercriminal has, for example, a state-level incentive to cause physical harm, it is possible through a care robot.

4.4 Cybercrime

The development of cybersecurity is a competition against cybercrime, where the analysis of various risk analyzes and motivational factors would lead to a better understanding of the factors behind the crime and potentially focus resources on the development of cybersecurity to address the most likely threats. The following are issues related to cybercrime that emerge from the interviews.

4.4.1 Ethics and morals

According to experts, cybercrime is viewed with blue eyes in Finland. People's attitudes towards cybercrime are affected by uncertainty about what is already possible in the field of cybercrime. The general belief is that people act ethically and thus do not want to cause harm to other people, especially the vulnerable.

4.4.2 Motivational factors

The motivating factors behind cybercrime emerge from all the interviews on several occurrences. Experts often consider different threats based on which motivational factors affect a criminal's actions and what benefits can be achieved from a criminal's perspective when a particular threat materializes. The general view of experts is that if a criminal has sufficient motivation and access to resources, the likelihood of various threats materializing will increase. At present, however, it is seen that care robotics is not yet such a tempting opportunity as to attract cybercriminals, as the benefits of crime are currently small. Experts have a hard time imagining why anyone at all would want to attack devices designed to help the vulnerable. However, the care robots of very significant persons can be exclusions.

4.4.3 Development of cybercrime

Experts are aware that cybercrime currently occurs in a variety of contexts. Although care robotics is not currently considered to be a particularly topical target for cybercrime, experts believe that where care robotics is evolving, cybercrime is also evolving.

5. Conclusions

The purpose of the paper is to map the experts' opinions on the cybersecurity threats and risks associated with care robotics. As the interviews progressed, saturation was observed in the research data, meaning that six interviews were sufficient for this study.

The use of care robots has the same risks and threats as the use of other ICT devices or robots, which supports the results of previous studies on the cybersecurity threats of care robots. The biggest threats are related to the hijacking of control of care robots, and the fact that they can be used for spying and eavesdropping, but other threats are also possible. In addition, network connectivity, and new features such as artificial intelligence and machine learning create more opportunities for cybercrime. In the future when the physical characteristics of robots, such as the ability to manipulate objects improve, threats to the physical environment will increase.

Although care robots have the same threats as other ICT devices already in use, there is a risk that care robots will be statistically less exposed to cybersecurity threats because there are few care robots. From this perspective, it seems that cybercrime is currently targeting other devices. However, the situation will change in the future as the use of care robots increases.

Care robotics as a robot class is so far very vague. At present, there are no rules or regulations that specifically stipulate that the safety and security of care robots must meet any requirements. If new devices that do not have a medical device classification are introduced, special attention should be paid to their cybersecurity. For example, if telepresence devices and other remote access robots are used for care, special care must be taken concerning their safety and security, as the experts interviewed in this study typically do not aim for a high level

of data security. If such devices are used for care, care must be taken to ensure that connections cannot be broken because sensitive conversations or the like may occur between the caregiver and the client.

Compared to previous studies, this study highlighted more aspects related to the human factors underlying cybersecurity, and that cybersecurity is a race against cybercrime. When deploying care robots and assessing their cybersecurity, it should be borne in mind that there is usually some motive behind criminal activity. If we assess risks narrowly (e.g., what worst can occur) and do not consider the motives behind the actions, we can conclude that there should be no care robots because they can cause things that are almost impossible to prevent. Using this logic, we could also conclude that there should be no cars because someone can sabotage the car so that it doesn't work as it should and the driver can crash. Therefore, the mapping of motives and the benefits of crime is key to striking a balance between acceptable and unacceptable risks in care robotics as well.

Further research is needed on the distribution of responsibilities related to the cybersecurity of care robots as more care robots are deployed; what kind of concept or entity ensures the safety and maintenance of the equipment throughout its life cycle, and how the responsibility should be divided between the different parties. This perspective should be further explored and mapped out what kind of service ecosystem would ensure the safety of care robots during development, deployment, and maintenance, and enable end-users to receive the guidance and support they need on the use of care robots.

Acknowledgements

This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 857159.

References

Dolic, Z., Castro, R. and Moarcas, A. (2019) "Robots in healthcare: a solution or a problem?, Study for the committee on environment, public health, and food safety", *Policy Department for Economic, Scientific and Quality of Life Policies,* European Parliament, Luxembourg.

Forum Virium (2020) "Hoivarobotti viihdytti muistisairaita ja helpotti hoitajien työtaakkaa Kustaankartanossa", [online], City of Helsinki 13.1.2020, https://www.hel.fi/uutiset/fi/helsinki/hoivarobotti-helpotti.

Fosch-Villaronga, E. and Golia, A. Jr. (2019a) "Robots, standards and the law: rivalries between private standards and public policymaking for robot governance", *Comput Law Secur Rev*, 35 (2) (2019), pp. 129-144

Fosch-Villaronga, E. and Golia, A. Jr. (2019a) "The intricate relationships between private standards and public policymaking in the case of personal care robots. Who cares more", in P. Barattini, F. Vicentini, G.S. Virk, T. Haidegger (Eds.), *Human-robot interaction: safety, standardization, and benchmarking*, CRC Press.

Fosch-Villaronga, E. and Mahler, T. (2021) "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots", *Computer law & security review* (41). DOI: 10.1016/j.clsr.2021.105528

Holder, C., Khurana, V., Harrison, F., Jacobs, L. (2016) "Robotics and law: key legal and regulatory implications of the robotics age (Part I of II)", *Comput Law Secur Rev,* 32 (3), pp. 383-402.

Lera, F., Llamas, C., Guerrero, Á., and Olivera V. (2017) "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety", *InTech Open*. DOI: 10.5772/intechopen.69796

Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. and Zanero, S. (2017) "An experimental security analysis of an industrial robot controller", *Proceedings of the 2017 IEEE symposium on security and privacy*, pp. 268-286.

Rousku, K. (2014) *Kyberturvaopas - Tietoturvaa kotona ja työpaikalla*, Talentum, Helsinki.

Schönberg, K. (2017) "Vanhukset ottavat robotin ilolla vastaan – hoitajat epäillen", [online], YLE, https://yle.fi/uutiset/3-9720927.

Särkikoski, T., Turja, T. and Parviainen, J. (2020) *Robotin hoiviin? Yhteiskuntatieteen ja filosofian näkökulmia palvelurobotiikkaan*, Vastapaino, Tampere.

Tzafestas, S. (2018) "Roboethics: Fundamental Concepts and Future Prospects", *Information,* 9 (148). DOI:10.3390/info9060148

Van Aerschot, L. and Parviainen, J. (2020) "Robots responding to care needs? A multitasking care robot pursued for 25 years, available products offer simple entertainment and instrumental assistance", *Ethics and Information Technology,* (22), pp. 247–256.

Vuorinen, S. (ed.) (2019) *Cyber security: Guidance for operators in the healthcare and social welfare sectors*. Publications of the Ministry of Social Affairs and Health, Helsinki.