Assessing Usability and Cybersecurity of AI Systems through the Human-Centered Design

Vita Santa Barletta[1], Miriana Calvano[1], Antonio Curci[1,2], C.M. Nadeem Faisal[1,3] and Antonio Piccinno[1]

[1]University of Bari Aldo Moro, Department of Computer Science, Bari, Italy
[2]University of Pisa, Department of Computer Science, Pisa, Italy
[3]National Textile University, Department of Computer Science, Faisalabad, Pakistan

Abstract

As Artificial Intelligence (AI) spreads in modern society, academia, companies, and governments are working towards the common goal of creating systems that are not just accurate, but that can be used by humans with efficiency, effectiveness, and satisfaction while respecting their rights and well-being. As the Human-Centered Design (HCD) establishes the processes that can be followed to reach this objective, other related challenges concern the privacy and security of those systems. This study investigates the impact that the HCD approach can have in the cybersecurity of AI systems to propose an approach that considers the different factors that can influence their evaluation and assessment, considering three main components: *Human-Computer Interaction*, *Cybersecurity*, and *Ethics and Law*.

Keywords

Artificial Intelligence, Cybersecurity, Ethics, Human-Centered Design, Usable Security

1. Introduction

Artificial Intelligence (AI) is permeating many aspects of our daily life, making it necessary to ensure that humans are fully considered in these systems' creation process, preserving their fundamental rights and preventing undesired events that can harm them [1]. The discussion concerning AI and, in general, technology is becoming more and more frequent, leading to the birth of novel legal frameworks that aim at regulating the way that these systems are created and used [2].

In the case of AI, multiple aspects must be considered by designers and developers concerning the accuracy of the models and their robustness, but there are other factors, no less important, that contribute to building those systems. In this regard, Human-Centered AI (HCAI) highlights how integrating the Human-Centered Design (HCD) approach is crucial to the creation of an AI system that is reliable, safe, and trustworthy [3, 4, 5]. The HCD approach stresses the involvement of users throughout the development process, ensuring that products meet their needs and capabilities [6]. Meeting these requirements translates into understanding their preferences, necessities, and cognitive models, which is not merely useful for the creation of usable User Interfaces (UIs), but rather in building interaction mechanisms that accommodate those needs, while not undermining the performance of the system.

This research work focuses on the cybersecurity of AI systems, specifically, how the HCD approach and the best practices belonging to Human-Computer Interaction (HCI) can improve users' privacy and security when using those systems. The goal is to investigate the field of Human-Centric CyberSecurity (HCCS), which incorporates a wide range of techniques and practices to improve cybersecurity through

Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.
vita.barletta@uniba.it (V. S. Barletta); miriana.calvano@uniba.it (M. Calvano); antonio.curci@uniba.it (A. Curci); nadeem.faisal@uniba.it (C.M. N. Faisal); antonio.piccinno@uniba.it (A. Piccinno)
https://serlab.di.uniba.it/people/vita-barletta (V. S. Barletta); https://ivu.di.uniba.it/people/calvano (M. Calvano); https://ivu.di.uniba.it/people/curci (A. Curci); https://ivu.di.uniba.it/people/faisal (C.M. N. Faisal); https://ivu.di.uniba.it/people/piccinno (A. Piccinno)
0000-0002-0163-6786 (V. S. Barletta); 0000-0002-9507-9940 (M. Calvano); 0000-0001-6863-872X (A. Curci); 0000-0001-8781-4143 (C.M. N. Faisal); 0000-0003-1561-7073 (A. Piccinno)

usability and User Experience (UX) [7]. These aspects should be considered from the development process's early stages to ensure that those systems are *secure-by-design* and consider *privacy-by-design* [8]. To guarantee that these needs are considered and integrated in the creation process, in 2016, the European Union (EU) enacted the General Data Protection Regulation (GDPR), which revolves around how users' data is used, stored, and processed, highlighting their fundamental rights [9]. It emphasizes the integration of privacy and data protection techniques in the development of systems, services, and products. This regulation is strictly connected with the European AI Act, which specializes in AI systems but also deals with their security, safety, and privacy [10, 9]. It is a legal framework that aims to regulate the creation, deployment, and use of AI in the EU, classifying systems in different risk categories [10]. Considering these aspects, the goal of this study is embodied in the following research question.

RQ: How is it possible to combine elements of HCI, Cybersecurity and Ethics in order to strengthen AI systems and safeguard humans?

The main goal is to create systems that support rather than replace humans, granting they better control over security and privacy, establishing a human-AI symbiotic relationship [11, 12]. In this study, we present preliminary considerations about the integration of these aspects into the cybersecurity of AI systems in order to comply with these standards. This article is structured as follows: Section 2 illustrates fundamental concepts of usability and security in AI systems while considering the legal landscape; Section 3 defines the essential elements for assessing the quality of AI systems considering usability, security and law proposing the human-centric cybersecurity approach; Section 4 sets out the conclusions.

2. Background Work

As previously mentioned, designers and developers must ensure that products comply with the requirements set by the necessities of their users, best practices, and legal obligations set by regulations such as the GDPR and the AI Act [9, 10]. In this context, the focus should also be put on the system's usability to provide users clear information about potential threats and to avoid misinterpretation that can compromise both user safety and data security [13].

This section presents considerations about the intersection among AI, cybersecurity and law, referring to these regulations.

2.1. Regulations and Frameworks for AI and Cybersecurity

The GDPR focuses primarily on the security of users' data when dealing with technology. Although this regulation does not focus on AI explicitly, there are some articles that can be relevant for AI developers, who must consider the high computational power of modern models and algorithms, for example, when processing personal data. Regardless of the type of technology, it is mandatory to guarantee the protection of users' privacy and human rights [14].

In this regard, Article 15 of the AI Act plays an important role, touching on cybersecurity issues for high-risk AI systems, as well as robustness and accuracy [15]. Although there exist established standards, rules, and guidelines for generic systems concerning cybersecurity, its implementation by design in AI-based systems is yet to be fully investigated. As the latter classifies AI systems based on a risk-based approach, the legal framework stresses the importance of cybersecurity for high-risk systems to protect users from undesired and unexpected events [16]. More specifically, some examples of high-risk systems are those used as a safety component of other products or if AI is itself the product, those that profile individuals. Thus, high-risk AI systems should be designed to be resilient against cyber-attacks, performed by exploiting the system's vulnerabilities, that can negatively alter their behavior and performance [16]. It is also important to refer to Article 9 of the AI Act, which focuses on the risk management process [15, 17]. It regulates risk management, a dynamic and continuous

process planned and executed throughout the lifecycle of a high-risk AI system. The management system aims to identify and manage, among other things, the known and foreseeable risks to health, safety, and fundamental rights. Throughout all phases of this process, it is mandatory to also focus on the implications that the technology has on individuals' data, which can impact their security and lead to undesirable and unlawful effects [17].

In this context, the cybersecurity of AI plays an important role: it aims to develop mature, safe and secure approaches and tools that can be used to secure AI models [18]. Many challenges exist in this new field due to the integration of AI; this leads to the emergence of AI-specific vulnerabilities and, consequently, it is necessary to follow standardized approaches and methodologies to face these threats [18, 19]. A first attempt to face this challenge is represented by the MITRE[1] corporation, providing a taxonomy and kill chain analysis about such AI-specific attacks, which is continuously updated based on new findings.

The use of AI presents several risks, including transparency in tracking model implementation as it is used as a black box, data sourcing issues and privacy violations. These challenges require a policy to manage cyber-AI risks [20]. This implies that cybersecurity is not a standalone requirement, but it is considered together with accuracy and robustness, which is the motivation behind the fact that Article 15 groups those three concepts together. To guarantee high-risk AI systems' compliance with the AI Act, a cybersecurity risk assessment must be performed before being spread on the EU market [16].

2.2. Usability and Security in AI systems

Implementing robust AI systems with intuitive user interfaces is one of the main concerns to address when creating AI systems in order to allow users to understand the system's functioning and detect malicious activities. In this scenario, usability and security contaminate each other resulting in the concept of *usable security*: security must be usable by persons with different expertise and systems must be usable while maintaining security, since in the absence of usable security, there is ultimately no effective security [13].

Usability and security are not considered two separate fields, but both are simultaneously addressed to build robust and secure systems that foster users' trust in the decision-making process, specifically when interacting with AI systems. In this context, humans are put at the center of the creation and interaction process, leading to building Human-Centered AI (HCAI) systems that align with humans' needs, preferences, and cognitive models, fostering a human-AI symbiotic relationship, improving both parties [21, 22].

2.3. Human Centric Cyber Security

Human-centric cybersecurity is an emerging approach that prioritizes individuals and their rights over traditional security-centric models [7]. This paradigm represents a shift in recognizing humans as both the weakest link and the best line of defense in cybersecurity [23]. It emphasizes the importance of understanding humans' cognitive models along with their vulnerabilities, behaviors, and decision-making processes within organizational contexts [23, 24]. As defined by Grobler et al., human-centric cybersecurity focuses on three main components:

- *User*: it is the individual who interacts with the systems for legitimate purposes. A user can exhibit varying levels of cybersecurity awareness because of various factors, ranging from demographics to past experiences [24].
- *Usage*: it concerns the functional aspects of both technological and non-technological measures to protect users from known security threats (e.g., spam detection algorithms, password-based authorizations, organizational policies, and cybersecurity internal laws) [24].
- *Usability*: it is the extent to which a system, product, or service is used by specified users to reach specified goals with effectiveness, efficiency, and satisfaction in specified contexts of use. When

[1] https://atlas.mitre.org/

it comes to cybersecurity, it is important to assess aspects that go beyond the mere technicalities [24].

3. Evaluating Usable Secure AI Systems

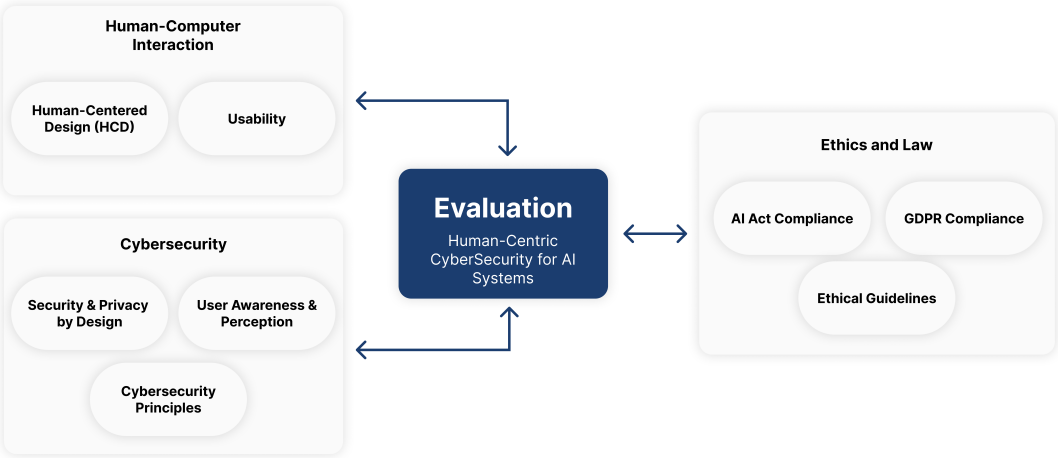

Figure 1: Approach for assessing and evaluating Human-Centered CyberSecurity in AI systems [25]

The evaluation of AI systems touches on multiple factors and disciplines, from the accuracy of the model to the interaction mechanisms that they are characterized by. In the current scenario, designers and developers must ensure their compliance with the legal frameworks that are emerging across the globe. We investigate an approach that revolves around the evaluation phase of AI systems, focusing on their security with respect to usability. Research in this area is increasingly moving towards this approach, especially within industrial organizations to achieve better results when it comes to individuals' security and privacy in the era of AI [23, 26, 27].

The approach proposed in this work is illustrated in Figure 1 and it is based on three main components: *Human-Computer Interaction (HCI)*, *Cybersecurity*, and *Ethics and Law* starting from an initial rapid review of the literature [25, 28, 29, 30, 24, 31]. It is crucial to identify user needs and context by understanding the specific needs, behaviors, and environment of the users, which can be achieved through foundation research (e.g. surveys, interviews and observations). Insights are translated into clear, actionable cybersecurity requirements, with features prioritized based on user feedback and threat analysis. Design research to create user-friendly interfaces and features helps users to manage security threats. The system is designed considering usability, security regulations, involving users in testing to gather feedback and improvements based on user experience and evolving threats while being compliant with the law. Finally, educating and supporting users is paramount, providing training and resources to help them understand and effectively use the system, and maintaining support channels for ongoing assistance and feedback.

The three components of the approach are described in the following sections.

3.1. Cybersecurity

Cybersecurity is characterized by the following aspects. It outlines the importance of ensuring the system's security and preserving privacy while considering users' awareness and perception.

Security and Privacy by Design Security by Design is an approach that emphasizes the need to consider security at every step of the development process, minimizing vulnerabilities and preventing malicious activities [32]. Privacy by Design (PbD) that emphasizes integrating privacy and data

protection into the development and operation of systems, services, and products [32]. The concept is centered around proactively embedding privacy from the design phase and at the organizational level.

User Awareness and Perception Training humans, especially in organizational scenarios, on cybersecurity practices to prevent human errors that could compromise security and their privacy. It is important to spread awareness concerning the methods, techniques, and guidelines that must be put in place in order to establish a secure and private environment [33].

Cybersecurity Principles The pillars of cybersecurity must be mapped with the other components of the approach. Taking into account the resources provided by the American's National Institute of Standards and Technology (NIST), other than the *CIA* Triad (Confidentiality, Integrity, Availability), the following principle must be included: Authentication and Authorization, Encryption, Vulnerability Management, Resilience, Monitoring and Logging, and Training[34].

3.2. Human-Computer Interaction

Human-Computer Interaction (HCI) is the discipline that studies methods and techniques to design and develop usable systems that can improve the interaction process [35]. Usability is the cornerstone of HCI, which can be ensured by creating systems following the HCD approach.

Usability It is critical because complex or unintuitive security measures often lead users to bypass them, weakening overall protection [36]. When systems are hard to use, people make errors, reuse passwords, or disable security features altogether. Effective cybersecurity must balance strong protection with ease of use to ensure users can comply without friction [37, 4].

Human-Centered Design It is an approach that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques [4].

3.3. Ethics and Law

The development and deployment of AI systems must align with existing regulatory and ethical frameworks to safeguard humans. In the European Union, laws and principles (i.e. AI Act and GDPR) guide the responsible use of AI, focusing on protecting individuals' rights and preventing potential risks.

European AI Act It is a law that regulates the development and use of AI in the European Union (EU) to ensure AI systems are safe and respect fundamental rights. It classifies AI systems in different categories of risk, including prohibited, high-risk, and those subject to transparency obligations. To create AI systems that are compliant with the AI Act, four principles must be referred to: protection, transparency, automation level and fairness [10].

GDPR It is a European legal framework that sets guidelines for the collection and processing of personal information from individuals. It applies to any organization that processes personal data of EU citizens, regardless of the organization's location, with the aim to safeguard people's privacy and sensitive data [9].

Ethics AI systems must not discriminate against individuals (e.g., minorities), exhibiting fair behavior and ensuring that biases are not perpetuated. These systems must also implement measures to prevent the malicious or dangerous use of AI, being safe and reliable. Social and Environmental Impacts must also be considered [38].

4. Discussions and Conclusions

The current state of this research presents a theoretical approach, but it is intended to validate it with practical hands-on AI systems. This approach finds relevant applicability in high-stakes scenarios, such as in the medical field, in which it is important that AI models properly access and processes data, complying with the ethical principles that guide the well-being in society [39]. In this domain, the adherence of an AI system to the security and legal standards holds equal importance to exhibiting a stable and accurate behavior [40]. This means that the model must support physicians in making decisions, but it also must be integrated with a system that features an interaction paradigm that fosters communication and learning. Such considerations imply that, when evaluating these systems, the field of HCI, Cybersecurity, and Ethics and Law must equally contribute with their own metrics, methods, and techniques [41, 21].

It is important to create secure and legally compliant systems while considering the challenges and opportunities of integrating AI into cybersecurity [42]. It is also crucial to keep humans at the center of the design, development, and evaluation of these systems, aligning to ensure safety, well-being, and robustness. As usability is becoming an increasingly central topic when it comes to AI systems, its connection to cybersecurity is not properly considered. At the same time, usable security principles and best practices must be integrated in such systems in their creation process [43]. The proposed approach involves attributing equal importance to HCI, cybersecurity, and Ethics and Law as a first effort to reach the higher objective of reaching a symbiotic relationship between humans and AI. This implies that, although humans are still the weakest link of the chain [13], AI systems can compensate for their limitations and enhance their cognitive capabilities [3].

Future works will concern the definition and validation of practical criteria that can be employed for evaluating AI-based systems adhering to HCCS that can be applied both in the academic and industrial contexts. Evaluating the approach will involve both its components and the AI systems taken in consideration; thus, case studies are necessary to ensure a scientific and technical soundness. The validation in will inevitably encompass the refinement and evaluation of the approach, which is currently theoretical, and iteratively improve it in order to achieve more standardization and systematization.

Acknowledgments

This work was partially supported by the following project: SERICS - “Security and Rights In the CyberSpace - SERICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] C. Sanderson, D. Douglas, Q. Lu, E. Schleiger, J. Whittle, J. Lacey, G. Newnham, S. Hajkowicz, C. Robinson, D. Hansen, AI Ethics Principles in Practice: Perspectives of Designers and Developers, IEEE Transactions on Technology and Society 4 (2023) 171–187. URL: http://arxiv.org/abs/2112.07467. doi:10.1109/TTS.2023.3257303, arXiv:2112.07467 [cs].

[2] G. Lazcoz, P. De Hert, Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities, Computer Law & Security Review 50 (2023) 105833. URL: https://linkinghub.elsevier.com/retrieve/pii/S0267364923000432. doi:10.1016/j.clsr.2023.105833.

[3] B. Shneiderman, Human-Centered AI, 1 ed., Oxford University PressOxford, 2022. URL: https://academic.oup.com/book/41126. doi:10.1093/oso/9780192845290.001.0001.

[4] ISO/TC 159/SC 4 Ergonomics of human-system interaction, Ergonomics of Human-System Interaction — Part 11: Usability: Definitions and Concepts, Standard ISO 9241-11:2018, International Organization for Standardization (ISO), 2018. URL: https://www.iso.org/standard/63500.html.

[5] C. N. Faisal, M. Gonzalez-Rodriguez, D. Fernandez-Lanvin, J. de Andres-Suarez, Web design attributes in building user trust, satisfaction, and loyalty for a high uncertainty avoidance culture, IEEE Transactions on Human-Machine Systems 47 (2016) 847–859.

[6] H. Susanto, F. Ibrahim, S. H. Nazmudeen, F. Mohiddin, D. Setiana, Human-centered design to enhance the usability, human factors, and user experience within digital destructive ecosystems, in: P. Ordóñez de Pablos, M. Lytras (Eds.), Global Challenges and Strategic Disruptors in Asian Businesses and Economies, IGI Global, 2021, pp. 76–94. doi:10.4018/978-1-7998-4787-8.ch005.

[7] R. J. Deibert, Toward a human-centric approach to cybersecurity, Ethics; International Affairs 32 (2018) 411–424. doi:10.1017/S0892679418000618.

[8] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, A visual tool for supporting decision-making in privacy oriented software development, in: Proceedings of the 2020 International Conference on Advanced Visual Interfaces, AVI '20, Association for Computing Machinery, New York, NY, USA, 2020. URL: https://doi.org/10.1145/3399715.3399818. doi:10.1145/3399715.3399818.

[9] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance), 2016.

[10] European Parliament, Council of the European Union, Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024.

[11] M. Alshamari, T. Alsalem, Usable ai: Critical review of its current issues and trends, Journal of Computer Science 19 (2023) 326–333. URL: https://thescipub.com/abstract/jcssp.2023.326.333. doi:10.3844/jcssp.2023.326.333.

[12] V. Santa Barletta, F. Cassano, A. Pagano, A. Piccinno, A collaborative ai dataset creation for speech therapies., in: CoPDA@ AVI, 2022, pp. 81–85.

[13] S. Garfinkel, H. R. Lipford, Usable Security: History, Themes, and Challenges, Synthesis Lectures on Information Security, Privacy, and Trust, 1 ed., Springer Cham, 2014. doi:10.1007/978-3-031-02343-9, published: 26 September 2014 for print, 01 June 2022 for eBook. Copyright Springer Nature Switzerland AG 2014. Part of the Synthesis Collection of Technology (R0), eBColl Synthesis Collection 5.

[14] European Parliamentary Research Service, The impact of the general data protection regulation (gdpr) on artificial intelligence, 2020.

[15] The European Parliament and the Council of the European Union, Artificial intelligence act, 2024. Unpublished legislation.

[16] H. Junklewitz, R. Hamon, A. André, T. Evas, J. Soler Garrido, J. I. Sanchez Martin, Cybersecurity of Artificial Intelligence in the AI Act, Publications Office of the European Union, Luxembourg, 2023. doi:10.2760/271009, jRC134461.

[17] J. Schuett, Risk management in the artificial intelligence act, European Journal of Risk Regulation (2023) 1–19. doi:10.1017/err.2023.1.

[18] C. Berghoff, J. Böddinghaus14, V. Danos, G. Davelaar13, T. Doms, H. Ehrich, A. Forrai, R. Grosu, R. Hamon10, H. Junklewitz10, et al., Towards auditable ai systems, in: Proceedings of the Auditing AI-Systems: From Basics to Applicat.(Workshop at Fraunhofer Forum), 2020.

[19] C. Baylon, C. Berghoff, S. Brunessaux, L. Burdalo, G. D'Acquisto, E. Damiani, S. Herpig, C. Louveaux, J. Mistiaen, D. C. Nguyen, et al., Securing machine learning algorithms (2021).

[20] A. Carlo, N. P. Mantı, B. A. S. WAM, F. Casamassima, N. Boschetti, P. Breda, T. Rahloff, The importance of cybersecurity frameworks to regulate emergent ai technologies for space applications, Jour-

nal of Space Safety Engineering 10 (2023) 474–482. URL: https://www.sciencedirect.com/science/article/pii/S2468896723000678. doi:https://doi.org/10.1016/j.jsse.2023.08.002.

[21] M. Calvano, A. Curci, G. Desolda, A. Esposito, R. Lanzilotti, A. Piccinno, Building symbiotic ai: Reviewing the ai act for a human-centred, principle-based framework, 2025. URL: https://arxiv.org/abs/2501.08046. arXiv:2501.08046.

[22] G. Desolda, A. Esposito, R. Lanzilotti, A. Piccinno, M. F. Costabile, From human-centered to symbiotic artificial intelligence: A focus on medical applications, Multimedia Tools and Applications (2024). URL: https://rdcu.be/d1RF4. doi:10.1007/s11042-024-20414-5.

[23] P. L. Morgan, P. M. Asquith, L. M. Bishop, G. Raywood-Burke, A. Wedgbury, K. Jones, A new hope: Human-centric cybersecurity research embedded within organizations, in: A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust, Springer International Publishing, Cham, 2020, pp. 206–216.

[24] M. Grobler, R. Gaire, S. Nepal, User, usage and usability: Redefining human centric cyber security, Frontiers in big Data 4 (2021) 583723.

[25] M. Maguire, Context of use within usability activities, International journal of human-computer studies 55 (2001) 453–483.

[26] M. B. Chhetri, X. Liu, M. Grobler, T. Hoang, K. Renaud, J. McIntosh, Report on the 2nd workshop on human centric software engineering & cyber security, SIGSOFT Softw. Eng. Notes 47 (2022) 12–14. URL: https://doi.org/10.1145/3520273.3520278. doi:10.1145/3520273.3520278.

[27] V. S. Barletta, F. Caruso, T. Di Mascio, F. Greco, T. Islam, V. Rossano, H. Xiao, Cybersecurity education for industry and academia (cse4ia 2024), in: Proceedings of the 2024 International Conference on Advanced Visual Interfaces, AVI '24, Association for Computing Machinery, New York, NY, USA, 2024. URL: https://doi.org/10.1145/3656650.3660536. doi:10.1145/3656650.3660536.

[28] A. Alarifi, M. Alsaleh, N. Alomar, A model for evaluating the security and usability of e-banking platforms, Computing 99 (2017) 519–535.

[29] A. Constantinides, M. Belk, C. Fidas, R. Beumers, D. Vidal, W. Huang, J. Bowles, T. Webber, A. Silvina, A. Pitsillides, Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations, ACM Transactions on Computing for Healthcare 4 (2023) 1–40.

[30] A. Nanda, J. J. Jeong, S. W. A. Shah, M. Nosouhi, R. Doss, Examining usable security features and user perceptions of physical authentication devices, Computers & Security 139 (2024) 103664.

[31] A. Kovačević, N. Putnik, O. Tošković, Factors related to cyber security behavior, IEEE Access 8 (2020) 125140–125148.

[32] C. Del-Real, E. De Busser, B. van den Berg, Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review, Computer Law Security Review 52 (2024) 105933. URL: https://www.sciencedirect.com/science/article/pii/S0267364923001437. doi:https://doi.org/10.1016/j.clsr.2023.105933.

[33] R. Beuran, D. Tang, Z. Tan, S. Hasegawa, Y. Tan, Y. Shinoda, Supporting cybersecurity education and training via LMS integration: CyLMS, Education and Information Technologies 24 (2019) 3619–3643. URL: http://link.springer.com/10.1007/s10639-019-09942-y. doi:10.1007/s10639-019-09942-y.

[34] Joint Task Force Interagency Working Group, Security and Privacy Controls for Information Systems and Organizations, Technical Report, National Institute of Standards and Technology, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. doi:10.6028/NIST.SP.800-53r5, edition: Revision 5.

[35] R. Polillo, Facile da usare: Una moderna introduzione all'ingegneria dell'usabilità, Apogeo Education, 2010.

[36] M. Saltarella, G. Desolda, R. Lanzilotti, V. S. Barletta, Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review, International Journal of Human–Computer Interaction 40 (2024) 4465–4483. URL: https://www.tandfonline.com/doi/full/10.1080/10447318.2023.2219964. doi:10.1080/10447318.2023.2219964.

[37] M.-A. Kaufhold, T. Mentler, S. Nestler, C. Reuter, The tension of usable safety, security and privacy, i-com (2025). URL: https://www.degruyter.com/document/doi/10.1515/icom-2025-0009/

html. doi:10.1515/icom-2025-0009.
[38] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.
[39] C. Mennella, U. Maniscalco, G. De Pietro, M. Esposito, Ethical and regulatory challenges of AI technologies in healthcare: A narrative review, Heliyon 10 (2024) e26297. URL: https://linkinghub.elsevier.com/retrieve/pii/S2405844024023284. doi:10.1016/j.heliyon.2024.e26297.
[40] F. Li, N. Ruijs, Y. Lu, Ethics & AI: A Systematic Review on Ethical Concerns and Related Strategies for Designing with AI in Healthcare, AI 4 (2022) 28–53. URL: https://www.mdpi.com/2673-2688/4/1/3. doi:10.3390/ai4010003.
[41] P. Goktas, A. Grzybowski, Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI, Journal of Clinical Medicine 14 (2025) 1605. URL: https://www.mdpi.com/2077-0383/14/5/1605. doi:10.3390/jcm14051605.
[42] I. Chomiak-Orsa, A. Rot, B. Blaicke, Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain, in: N. T. Nguyen, R. Chbeir, E. Exposito, P. Aniorté, B. Trawiński (Eds.), Computational Collective Intelligence, volume 11684, Springer International Publishing, Cham, 2019, pp. 406–416. URL: http://link.springer.com/10.1007/978-3-030-28374-2_35. doi:10.1007/978-3-030-28374-2_35, series Title: Lecture Notes in Computer Science.
[43] M. Calvano, A. Curci, R. Lanzilotti, A. Piccinno, The human-centered approach to design and evaluate symbiotic ai systems, in: Proceedings of the 1st International Workshop on Designing and Building Hybrid Human-AI Systems co-located with 17th International Conference on Advanced Visual Interfaces (AVI 2024), Arenzano, Genoa, 2024.