Human Rights education as a Component of the European Union cybersecurity curricula

Maria Teresa Baldassarre [1], Berenice Fernández Nieto [1,2]*, and Azzurra Ragone [1]

[1] *Università degli Studi di Bari, Via Edoardo Orabona, 4, 70125 Bari, Italy*
[2] *Scuola IMT Alti Studi Lucca, Piazza S.Francesco, 19, 55100 Lucca LU*

Abstract

The training of professionals in the field of cybersecurity is a pressing need that multiple countries are working to meet. Currently, most of curricula place a significant emphasis on technical, economic, legal, and national security concerns. Nevertheless, it is essential to incorporate a human-centered approach that brings the social dimension into cybersecurity education plans and highlights the relevance of preserving human and digital rights in an era of constant and rapid change. To this end, this paper seeks to diagnose the current state of the curricula in the field of cybersecurity to identify trends in the training profiles and knowledge gaps regarding human rights formation.

Keywords

Cybersecurity education, human rights, digital rights, Human-centered cybersecurity

1. Introduction

Training cybersecurity professionals is a critical global need as cybersecurity threats increase in frequency and complexity. According to data for 2022, the economic impact of cyber-attacks on the private sector was at least USD 100,000 [1]. Meanwhile, a 2019 survey of cybersecurity professionals in Europe revealed a shortage of approximately 291,000 professionals, a significant increase from the previous year when the demand for professional staff was estimated at 142,000 [2].

While the professional field of cybersecurity is expanding, it demands holistic and multidisciplinary approaches that consider the social impact of technologies and the potential risks of activities that protect and regulate cyberspace. Protecting cyberspace entails more than just safeguarding information systems; it also entails ensuring that individuals' rights are upheld. As in the case of facial recognition technologies, there are several cases where new protection measures violate the rights of specific populations. Events like these highlight the importance of a comprehensive profile capable of developing safeguards for individuals' rights.

According to the Council of Europe and the Charter on Education for Democratic Citizenship and Human Rights Education, the Education for Democratic Citizenship and Human Rights contributes to the training and awareness of professionals with knowledge, skills, and behaviors that contribute to the construction and defense of a universal culture of human rights in society, as well as the promotion and protection of fundamental freedoms [3]. As a result, this responsibility must prevail in the cybersecurity field.

Given these challenges, we want to conduct a comparative and descriptive analysis of current curricula in the European Union to assess the state of the art in cybersecurity educational programs. We will identify, collect, and analyze undergraduate and postgraduate program content to determine the

IS-EUD 2023: 9th International Symposium on End-User Development, 6-8 June 2023, Cagliari, Italy
* Corresponding author
EMAIL: mariateresa.baldassarre@uniba.it (M.T. Baldassarre); b.fernandeznieto@studenti.uniba.it (B. Fernández Nieto); azzurra.ragone@uniba.it (A. Ragone)
ORCID: 0000-0001-8589-2850 (M.T. Baldassarre); 0009-0007-0468-5050 (B. Fernández Nieto); 0000-0002-3537-7663 (A. Ragone)

dominant orientation. In addition, a survey of education professionals, institutions, and centers will be conducted to ascertain their perspectives on the need for a human-centered approach to cybersecurity expert training. This research is motivated by the need to bridge the gap between the growing demand for cybersecurity professionals and the need to emphasize human rights education.

The paper is organized as follows: Section 2 explains the different dimensions of the problems, boundaries, and challenges; Section 3 describes the Research Questions (RQs) and the methodology we will follow to answer these RQs; Section 4 highlights the goals and objectives we want to pursue in this systematic study.

2. Human Rights in cybersecurity curricula

Awareness of human rights tends to be addressed superficially within cybersecurity curriculums. Currently, and in light of the proliferation of educational programs, it is essential to open spaces for training on human and digital rights. We must acknowledge that human rights are universal and inherent in all people, regardless of gender, nationality, ethnicity, religion, or language [4], and nowadays, they are also exercised by digital means.

New technologies are relevant to human rights, and it has been acknowledged that they amplify their reach and exercise; consequently, all activity aimed at regulating and protecting cyberspace has an inescapable effect on human rights. It is important to note that there are also rights that depend heavily on the internet as the "digital rights," which are the result of technology-enabled ways to be and act. Digital rights include rights such as freedom of expression, access to information, privacy, equality, inclusion, and non-discrimination, among others [5], [6].

In this scenario, it is worth re-considering a contentious issue within security studies: security for whom? This question invites us to reflect on who we consider when discussing cybersecurity. In the educational-training field of cybersecurity, we need to examine to which extent it has incorporated a human-centered perspective or if we are only looking at the systems [7]. The exercise is urgent since the absence of a human rights focus risks training professionals unaware of digital activities' impact on people and vulnerable populations and how people's rights are currently violated in authoritarian regimes in the name of security[8].

In this scenario, it is worth re-considering a contentious issue within security studies: security for whom? This question invites us to reflect on who we consider when discussing security. In the educational-training field of cybersecurity, we need to examine to which extent it has incorporated a human-centered perspective or if we are only looking at the systems. The exercise is urgent since the absence of a human rights focus risks training professionals unaware of digital activities' impact on people and vulnerable populations and how people's rights are currently violated in authoritarian regimes in the name of security [9].

In 2022 the European Union Agency for Cybersecurity (ENISA) published a paper identifying the training plans for cybersecurity professionals in European Union. Italy, Greece, the Czech Republic, Spain, Ireland, the Netherlands, Luxembourg, Malta, Estonia, France, Slovenia, Portugal, Austria, and Switzerland are among the countries on the list [10]. ENISA figures also show a steady increase in cybersecurity programs (see graph below).

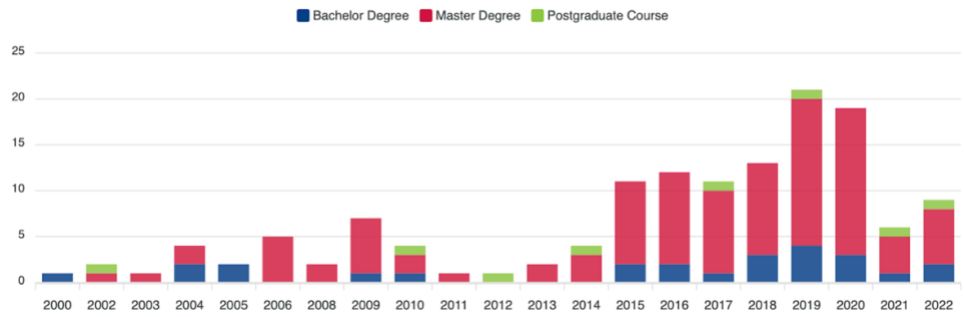

Figure 1. European Union Cybersecurity Programs Evolution [11]

The identified initiatives include ethical hacking challenges, training, and awareness platforms. Other studies, for example, Martti Lehto [12], examines national cybersecurity programs in Finland. The findings highlight the crucial role of cybersecurity research and development (R&D) and education in bolstering Finland's information security. At the regional level, a survey conducted by Blažič in 2021 identified skill gaps in cybersecurity education among higher education institutions in the European Union. This technical-focused analysis shed light on the educational requirements in various areas, including cryptography, networking, secure coding principles, operating system internals, proficiency with Linux-based systems, and more [13].

While informative and valuable, the analyses above primarily concentrate on technical skills within cybersecurity education at various educational levels. The social dimension, which encompasses broader aspects such as human behavior, ethics, legal frameworks, and social implications, has not been extensively addressed. Hence, there is a need to ensure a comprehensive and holistic approach to cybersecurity training.

The debate around human rights is unfolding on the theoretical side, where several analyses discuss the importance of finding a balance between cybersecurity and individual freedoms. Taddeo, for example, describes this equilibrium as "the struggle between liberties and authorities"[14]. Pagallo presents another study from the legal sphere, stating that "at least in Western legal systems, it should be clear that either civil rights prevail over cybersecurity (no balancing), or such balance has to satisfactorily protect individual rights (proportionality)" [15]. Pavlova also emphasizes the need for a human rights-based approach in cybersecurity and explores the apparent tradeoffs of sacrificing freedoms and rights for security. Her analysis calls for greater awareness and skill development to establish cybersecurity's human rights standards [16].

Most of the above-mentioned literature demonstrates the coexistence of two parallel approaches. On the one hand, there is a recognized need to develop and equip professionals in the field and meet the growing demand. On the other hand, there is an urgency to incorporate human rights approaches within cybersecurity. However, analyses that effectively converge these two needs are relatively scarce. This situation invites further exploration into a people-centered educational vision. Such an approach would emphasize the significance of not only technical expertise but also an understanding of the ethical, legal, and societal dimensions of cybersecurity.

In view of the aforesaid, our analysis aims to contribute to ongoing efforts to foster a people-centered perspective by raising awareness among cybersecurity students and practitioners, who will ultimately protect cyberspace in the coming years and recalibrate the direction towards a more human rights-based approach.

3. RQs and Methodology

The Research Questions (RQs) guiding the present proposal are: (RQ1) What is the state of the art of cybersecurity education programs in the European Union (EU)? (RQ2) Which perspectives

dominate the content of these programs? and (RQ3) How do education professionals, institutions, and centers perceive the necessity of a human-centered approach to training cybersecurity experts?

To answer the above-mentioned questions, we will adopt a mixed-methods approach that integrates qualitative and quantitative data collection and analysis techniques to address these inquiries. Our proposed methodology entails mapping cybersecurity programs and conducting a comparative analysis using documentary evidence. The methodology will be guided by Cambridge Assessment criteria [17], consisting of:

1. Define study aims and use
2. Determine curriculum selection criteria
3. Delimitation of the number of documents to analyze
4. Filter relevant documentation and sources of data
5. Determine the curriculum features that will be the basis of comparison
6. Consolidate findings through visual representation

In addition, we will perform a survey to gather insights from education professionals, institutions, and centers regarding incorporating a human-centered approach in training cybersecurity experts. The survey will be distributed electronically to a specifically targeted sample of individuals and organizations within the European Union. This phase will encompass the following steps:

1. Definition of distribution channels, target audience, and distribution timeframe
2. Survey design: We will carefully design a questionnaire to capture relevant perspectives and gather valuable information. Some questions could be:
   a) How important do you consider including interdisciplinary perspectives (e.g., psychology, sociology, law) in cybersecurity education?
   b) How familiar are you with the concept of digital rights?
   c) Are there any specific ethical or societal considerations that you believe should be addressed in cybersecurity education?
3. Survey distribution
4. Results analysis and visualization
5. Recommendations for public policy

Some of the limitations that may arise include: *i) time constraints* - the scope and available resources may impose limitations on the depth and breadth of the analysis, potentially preventing a comprehensive examination of all curricula and perspectives, and *ii) sample bias* - the survey responses and curricula analyzed may not fully represent the entire population, and the findings may be influenced by the characteristics and perspectives of the sampled individuals or organizations.

4. Prospects

The findings of this study could inform the development of new cybersecurity curricula emphasizing the ethical and social implications of cybersecurity and the significance of human rights protection in digital contexts. Our study could also encourage additional research on this field, such as studies examining the efficacy of different approaches to teaching and the effect of human-centered perspectives on the attitudes and behaviors of cybersecurity experts. The results could also contribute to implementing and promoting a comprehensive educational roadmap to promote human rights knowledge among cybersecurity professionals.

The analysis of human rights education as a component of European Union cybersecurity curricula has the potential to influence policy, curriculum development, international collaboration, and future research in the field. The findings could have far-reaching implications for cybersecurity education in the European Union and beyond.

5. Acknowledgements

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

6. References

[1] I. O'Sullivan, "Report: Cyberattacks Cost Most Businesses Over $100,000," *Tech.co*, Mar. 22, 2023. https://tech.co/news/cyberattacks-cost-businesses-over-100000 (accessed May 16, 2023).
[2] ENISA, "Cybersecurity Skills Development in the EU," *ENISA*, 2020. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (accessed May 16, 2023).
[3] Council of Europe, "Introducing human rights education - Manual for Human Rights Education with Young people - www.coe.int," *Manual for Human Rights Education with Young people*, 2023. https://www.coe.int/en/web/compass/introducing-human-rights-education (accessed May 16, 2023).
[4] Office of the United Nations High Commissioner, "¿Qué son los derechos humanos?," *OHCHR*. https://www.ohchr.org/es/what-are-human-rights (accessed May 16, 2023).
[5] European Commission, "What about digital rights?," *Living Democracy*, Nov. 08, 2022. https://www.living-democracy.com/what-about-digital-rights/ (accessed May 16, 2023).
[6] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, and M. Scalera, "Privacy Knowledge Base for Supporting Decision-Making in Software Development," in *Sense, Feel, Design*, C. Ardito, R. Lanzilotti, A. Malizia, M. Larusdottir, L. D. Spano, J. Campos, M. Hertzum, T. Mentler, J. Abdelnour Nocera, L. Piccolo, S. Sauer, and G. Van Der Veer, Eds., Cham: Springer International Publishing, 2022, pp. 147–157. doi: 10.1007/978-3-030-98388-8_14.
[7] V. S. Barletta, F. Cassano, A. Pagano, and A. Piccinno, "New perspectives for cyber security in software development: when End-User Development meets Artificial Intelligence," in *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Sakheer, Bahrain: IEEE, Nov. 2022, pp. 531–534. doi: 10.1109/3ICT56508.2022.9990622.
[8] C. Catalano, A. Chezzi, M. Angelelli, and F. Tommasi, "Deceiving AI-based malware detection through polymorphic attacks," *Comput. Ind.*, vol. 143, p. 103751, Dec. 2022, doi: 10.1016/j.compind.2022.103751.
[9] M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, and M. Scalera, "Teaching Cyber Security: The HACK-SPACE Integrated Model," presented at the Italian Conference on Cybersecurity, 2019. Accessed: May 18, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Teaching-Cyber-Security%3A-The-HACK-SPACE-Integrated-Baldassarre-Barletta/2cdd4024bd77d4bfdded094a3f0c8c2bcfda3cf3
[10] European Union Agency for Cybersecurity., *Cybersecurity education initiatives in the EU Member States: December 2022*. LU: Publications Office, 2023. Accessed: May 16, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/486119
[11] ENISA, "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*. https://www.enisa.europa.eu/topics/education/cyberhead (accessed May 16, 2023).
[12] I. R. Management Association, Ed., *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2018. doi: 10.4018/978-1-5225-5634-3.
[13] B. J. Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training," *Technol. Soc.*, vol. 67, p. 101769, Nov. 2021, doi: 10.1016/j.techsoc.2021.101769.
[14] M. Taddeo, "Cyber Security and Individual Rights, Striking the Right Balance," *Philos. Technol.*, vol. 26, no. 4, pp. 353–356, Dec. 2013, doi: 10.1007/s13347-013-0140-9.
[15] U. Pagallo, "Online Security and the Protection of Civil Rights: A Legal Overview," *Philos. Technol.*, vol. 26, no. 4, pp. 381–395, Dec. 2013, doi: 10.1007/s13347-013-0119-6.
[16] P. Pavlova, "Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups," *Peace Hum. Rights Gov.*, vol. 4, no. 11/2020, pp. 391–418, 2020, doi: 10.14658/pupj-phrg-2020-3-4.

[17] J. Greatorex, N. Rushton, T. Coleman, E. Darlington, and G. Elliott, “Towards a Method for Comparing Curricula,” University of Cambridge Local Examinations Syndicate (Cambridge Assessment), Jul. 2019.