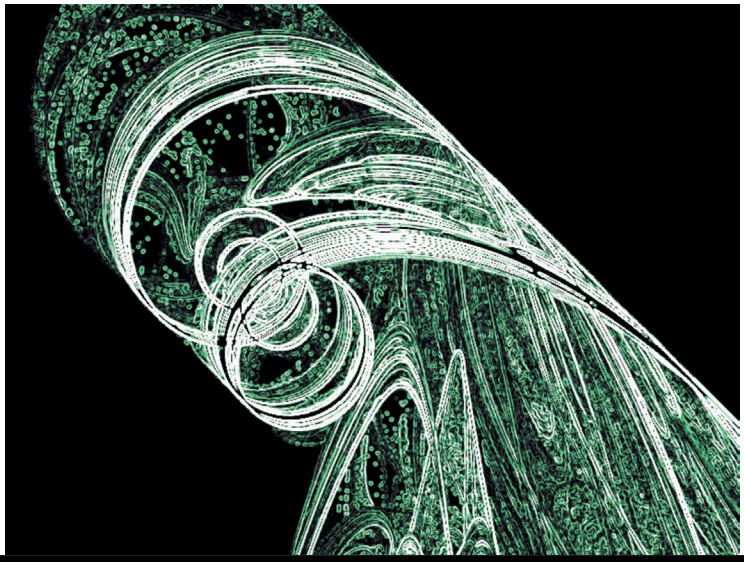
Management in Digitals Times 3

Krzysztof Wasilewski

Digital Humanities and Digital Skills in the Future of Work



PETER LANG

Krzysztof Wasilewski

Digital Humanities and Digital Skills in the Future of Work

The volume covers the field of digital humanities regarding the future of work. What digital skills will be needed in the nearby future? How digitization and digitalization change the very nature of science and the workplace? The authors represent higher education institutions which form the EU4Dual European University, as well as associated Ukrainian universities. Therefore the papers are often a result of applied and cooperative research, done together with the industry. As such they focus on practical usage of digital humanities and digital skills.

The Author

Krzysztof Wasilewski is an associate professor of media studies and political science at the Koszalin University of Technology, Poland where he leads the Digital Humanities and New Media Lab; his current research interests include digital humanities, new media and collective memory, heritage studies.

ISBN 978-3-631-92448-8

www.peterlang.com

Digital Humanities and Digital Skills in the Future of Work

MANAGEMENT IN DIGITAL TIMES

Edited by Piotr Olaf Żylicz

VOLUME 3

Krzysztof Wasilewski

Digital Humanities and Digital Skills in the Future of Work

PETER LANG
Berlin · Bruxelles · Chennai · Lausanne · New York · Oxford

Bibliographic Information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.d-nb.de.

Library of Congress Cataloging-in-Publication Data

Names: Wasilewski, Krzysztof, editor.
Title: Digital humanities and digital skills in the future of work / Krzysztof Wasilewski.
Description: New York : Peter Lang, [2025] | Series: Management in digital times, 2194-5918 ; 3 | Includes bibliographical references.
Identifiers: LCCN 2025002363 (print) | LCCN 2025002364 (ebook) | ISBN 9783631924488 (print) | ISBN 9783631924495 (e-book) | ISBN 9783631934777 (e-pub)
Subjects: LCSH: Humanities--Electronic information resources. | Humanities--Computer network resources. | Work. | Computer literacy. | Labor supply--Effect of technological innovations on.
Classification: LCC AZ195 .D54122 2025 (print) | LCC AZ195 (ebook) | DDC 001.30285--dc23/eng/20250317
LC record available at https://lccn.loc.gov/2025002363
LC ebook record available at https://lccn.loc.gov/2025002364

Cover illustration: Courtesy of Benjamin Ben Chaim.
Cover Design by Peter Lang Group AG

NAWA NARODOWA AGENCJA WYMIANY AKADEMICKIEJ

KOSZALIN UNIVERSITY OF TECHNOLOGY

LABORATORY DIGITAL HUMANITIES AND NEW MEDIA
Koszalin University of Technology

EU4Dual
The European Dual Studies University

This publication has been supported by the Polish National Agency for Academic Exchange under the task assigned by the Ministry of Education and Science Republic of Poland Solidarity with Ukraine - European Universities.

This publication is a result of the Lighthouse Research Initiative "Interdisciplinarity in Social Sciences. A European Way of Life", led by the Koszalin University of Technology – Digital Humanities and New Media Lab, within the EU4Dual European University.

ISSN 2699-3511
ISBN 978-3-631-92448-8 (Print)
ISBN 978-3-631-92449-5 (E-PDF)
ISBN 978-3-631-93477-7 (E-PUB)
DOI 10.3726/b22730

PETER LANG Open

Published by Peter Lang GmbH, Berlin (Germany)
info@peterlang.com – www.peterlang.com

This publication has been peer reviewed.

Contents

Krzysztof Wasilewski*

Digital Humanities and Digital Skills in the Future of Work: Introduction

Abstract: The aim of this paper is to analyze the future of work through the prism of digital skills and digital humanities. As such, it constructs a framework for further investigation into various aspects of the workplace in the ever changing conditions. As digital skills are considered to be key elements of the future employee's portfolio, digital humanities offers an interdisciplinary space for developing them. The author proposes a modified definition of digital humanities, which focuses less on its academic potential and more on its ability to combine human-centric approach with digital skills. By promoting collaboration, data analysis and communication, digital humanities is a crucial element of the future of work.

Keywords: digital humanities, digital skills, future of work, data analysis, collaboration

What is the future of work? Among the plethora of definitions of this concept, it is difficult to find one that would suit everyone. One might say the same about digital humanities and digital skills, which are commonly associated with the future of work. It turns out that before deciding what the work will be in a decade, first some work must be done now in order to set the frames of any further discussion in this field. One of the few academic papers researching the future of work (Rosati, Conway, van der Werff, 2023) notices that:

> The term 'Future of Work' in itself poses at least three significant challenges for researchers, practitioners and policymakers alike. Firstly, the study of the future requires boundaries. Predicting the future in the social sphere is particularly difficult as there are no strong laws (as in the sciences), and identifying and aggregating relevant information is complicated by its dispersal across different people and organizations.

Popular and academic texts about the future always carry the danger of becoming obsolete before they are even published. It is enough to think about scholarly predictions from the 1990s, which perceived the development of the internet as a revolutionary force that would impact work in particular and globalization in general. Most of them were proved wrong as soon as 1998, when the so-called "dot-com bubble" burst. Others provided leading companies with myths "readily

* *Digital Humanities and New Media Lab, Faculty of Humanities, Koszalin University of Technology, ORCID: 0000-0002-5378-2822*

available in the wider American culture of the time" to "manipulate their employees" (Tapia, 2004). Again, whatever was thought about the future of work in the second half of the 2000s was placed in the dustbin of history by the 2008 global economic crisis. Before 2020 home office seemed like a marginal form of contemporary work environment. By the end of March 2020 it became the standard, much like an eight-hour workday in the 20th century. And it has remained as such even long after the Covid-19 pandemics reached its apogee in late 2021.

The advent of the AI age makes any predictions even less reliable. Paradigms that set the scope of our understanding of work and its future seem to be no longer useful:

> Today advances in technology are changing the demand for skills at an accelerated pace. New technologies can not only handle a growing number of repetitive and manual tasks but also perform increasingly sophisticated kinds of knowledge-based work—such as research, coding, and writing—that have long been considered safe from disruption (Doumi et al., 2023).

There is a growing consensus that we are living in the times of disruption. The reason lies not only in technological breakthroughs, but also political, social, and economic changes that have been taking place all over the world in the 21st century. Unsurprisingly any discussion on the future of work must be limited to general outlook while some of the key categories of the contemporary discourse are reskilling and adaptability. Around these categories its own prediction about the future of work provides the McKinsey Global Institute, one of the leading think-tanks of economic and business development. In a report published in early 2023, it lists expected outcomes of the workplace in the upcoming years. Among them are: reskilling, job-growth limited to high-skill jobs, decline of job offers in traditional occupations, such as clerks and office workers, remote work, further development of e-commerce, and the growing need for adaptation of digital technologies (De Smet, Ellingrud, Smit, 2023).

At the same time, work in the future will be shaped not only by technological developments, but - as it has already been underlined - by political, social, and cultural tensions. In its scoping paper from April 2024, the Organization for Economic Cooperation and Development (OECD) maintains that among non-technological key factors in the future of work are climate change migrations and "evolving geography". According to OECD:

> Understanding the impact of migration on the labour market is key to designing efficient labour migration and integration policies. The impact of immigration on wages and employment depends on a variety of factors, such as the skills of immigrants, their concentration across regions, occupations and industries, as well as the local labour market conditions.

In the times of technological, political, social, and economic change it is easy to forget that the future of work is about people. Whatever problems will be solved - or created - by AI and other digital tools, they should be considered from the perspective of human well-being. This is why in the "9 trends that will shape work in 2024 and beyond", Harvard Business Review cites a research that focuses on those aspects whose goal is to improve the position of employees. In their paper, McRae, Aykens, Lowmaster and Shepp (2024) list the following trends - all of which prioritize people over technology:

1. Organizations will offer creative benefits to address the costs of work
2. AI will create, not diminish, workforce opportunity
3. Four-day workweeks will move from radical to routine
4. Employee conflict resolution will be a must-have skill for managers
5. GenAI experiments will yield hard lessons and painful costs
6. Skills requirements will overtake degree requirements as the "paper ceiling" crumbles
7. Climate change protection becomes a new employee benefit
8. DEI won't disappear; it will become more embedded in the way we work
9. Traditional stereotypes of career paths will collapse in face of workforce change

As such, the future of work provides both a threat and opportunity for contemporary and prospective workforce. On the one hand, in many scenarios, experts maintain that technological progress, especially the development of AI, will reduce the number of job offers, leaving many people unemployed. Experts suggest that AI may replace some 300 million full-time jobs by 2030 (Talmage-Rostron, 2024). On the other hand, the European Union and other political bodies try to build "an economy that works for people". As early as 2020, the European Commission introduced the concept of a strong social Europe for just transition. The plan comprises 20 principles divided into three chapters: Equal opportunities and access to the labor market, Fair working conditions, Social protection and inclusion. This European approach combines the need for technological development and innovation embracement with putting humans at the center of these changes.

The future of work is, then, the future of humans. And this is closely associated with digital skills. According to a paper published by the Digital Skills & Jobs Platform, an official website of the European Union:

> If we take a look at labour market trends, we can see that the digital transition has brought up specific needs and transformed many occupations and tasks. Most jobs today require some level of digital skills, including even those that do not ask for high levels of qualifications or experience - like working in a warehouse or as shop assistant, checking stock and inventory. Increasingly, the work of other specialists with higher

> qualifications in their respective disciplines, is now also dependent on digital skills: biologists need to work with complex digital 3D representations of molecule structures, lawyers now consult big juridical databases to study precedents and all aspects of legislation (Sanz, 2023).

In academic discourse on digital skills there is a consensus on how they will impact the future of work. What is more, digitization is going to change those skills, which traditionally were not associated with the process of digitization, such as: communication skills, collaboration skills, creativity or critical thinking (Laar et al., 2020). As Lang and Triantoro (2022) maintain:

> The future of work depends on digital skills. Governments, businesses, and educational institutions need to collaborate and make significant investments to address the digital skills crisis, which is a gap between necessary digital skills and available digital skills. Approximately 90% of jobs in developed economies require some level of digital skills, while one third of the labor force has a limited ability to use digital skills productively.

It is thus not surprising that the European Union considers the development of digital skills to be a crucial element of its strategy for ensuring technological sovereignty. According to the Digital Decade Policy Programme (DDPP), "basic digital skills are a precondition for inclusion and participation in the labour market and society. Furthermore, a strong digital economy powered by Europeans with digital skills is vital for innovation, growth, jobs, and European competitiveness" (DDPP). Among the objectives of the Digital Decade are a digitally skilled population and highly skilled digital professionals, secure and sustainable digital infrastructure, digital transformation of business, and digitalization of public services. Although other countries, especially the United States, Canada, Australia, Japan, and China prioritize digital skills in their educational and economic policies, the European Union seems to be the leader in absorbing the real impact of digitization in personal and professional development (DPPP).

Although several steps have been taken, reaching the 2030 objectives requires even more effort. What is the most striking is the fact that still a considerable percentage of the EU population lacks basic digital skills, such as using the computer and simple software. Another problem is little awareness of online security among various age groups. According to the Report on the State of the Digital Decade 2024:

> Very significant work remains to be done to reach the 2030 targets on digital skills: only 55.6% of EU's population has at least basic digital skills and, at the current pace, the number of ICT specialists will reach just 12 million by 2030 – well below the EUR 20 million target and amid growing competition for digitally skilled talent. The annual progress achieved in 2023 is alarmingly insufficient, falling between 2.5 and 3 times less than the rate needed to reach the targets by 2030 (European Commission, 2024).

The significance of digital skills in the future of work is reflected by the European Commission's call on member states to take some significant measures leading to the 2030 targets. Among them, the commission specifically highlighted the following: integration of digital technologies into teaching and empowering teachers to use them, supporting the development of digital educational tools, including research into the impact of artificial intelligence, taking cybersecurity measures in education and training, including awareness raising, investing in connectivity, digital infrastructure and digital accessibility in education and training.

Among others, this situation requires a new approach to higher education. More and more higher education institutions (HEIs) move from traditional bachelor and master's programs to microcredentials, which seem to answer the current need of the life-long-learning paradigm. Considering that digital skills are prone to constant changes and modifications, these short-term courses have the potential to provide students with the up-to-date qualifications and serve as support for more classic education. In addition to this, HEIs offer flexible online courses and digital learning platforms that allow students to develop digital skills at their own pace (Carabregu-Vokshi et al., 2024). Institutions can also adopt hybrid models that combine in-person and virtual learning experiences. In a paper published under auspices of the European Universities Association (EUA) on digital skills, Jørgensen (2019) points out that:

> As the digital transformation is moving ahead, the question of digital skills has become a societal challenge: are people equipped with the right skills to make use of the new possibilities in their work and, in a larger sense, as citizens? Labour markets are changing due to automatisation. The need for mid-skilled labour has decreased while that for high-skilled labour, often university graduates, has increased over the last decades.

As a result, universities, together with other higher education institutions, must include digital skills in their curriculums in all fields of study. It can be observed among universities around the world that relevant digital competencies, such as data analysis, programming, or digital marketing are integrated into all fields of study—whether it's business, humanities, or the sciences. Moreover, future engineers are expected to blend technical skills (like coding, digital design, or data analytics) with soft digital skills, such as critical thinking about technology, ethical use of digital tools, and digital collaboration.

One of the direct efforts taken by the European Union and HEIs of member states is the call for proposals on advanced digital skills whose objective is to "to support excellence in higher education institutions, making them world leaders in training the digital specialists of the future and to increase the capacity of the educational offer in the area of advanced digital skills. This should lead to the

development of dynamic digital educational ecosystems where higher education institutions as well as innovative partners from industry and research work together to attract and retain the best talents worldwide" (). This and other examples show the growing awareness - not only in Europe - of the role of digital skills in the future of work. If digitization, together with AI, seems to be the main theme of both business and political discourse, then digital skills (in all their forms) set the frames not only for theoretical discussions, but first and foremost for educational efforts.

The last element of this triangle - beside the future of work and digital skills - is composed by digital humanities (DH). As experts maintain that digital skills are not enough if they are not supported by soft skills, such as communication, leadership or empathy, digital humanities offers ways to combine them (Svensson, 2016). What originated as a field within literature studies and (to a lesser extent) history, has evolved into a paradigm that paves the way for humanities and social sciences in applied, socially-oriented research (Brennan, 2018). Although - as it has been mentioned in the first paragraph, digital humanities has earned a plethora of definitions (Gold, 2012). One of the most popular one states that DH is:

> … a diverse and still emerging field that encompasses the practice of humanities research in and through information technology, and the exploration of how the humanities may evolve through their engagement with technology, media, and computational methods (Alliance of Digital Humanities Organizations).

However, in approaching the future of work, I propose to modify this definition by prioritizing the engagement with technology and computational media instead of humanities research. As such, humanities research would be not the final goal but a means to help people acquire digital skills. What is more, digital humanities may help people better understand their role in a digitized world. Linking DH with the contemporary need for digital skills in the labor market should emphasize the interdisciplinary nature of the digital humanities and the transferable skills it fosters. As a result, key issues of digital humanities should be:

1. Skill development in digital tools and methods
2. Critical thinking and problem-solving
3. Content creation and digital storytelling
4. Preservation and curation of knowledge
5. Human-centered and socially-responsible digital technologies
6. Soft skills in a digitized world

Based on literature review and available definitions of DH, it can be stated that the field involves the use of sophisticated tools for such activities as textual analysis,

data visualization, and metadata curation (Rahaman, 2018). Although they are first and foremost research methods and techniques used by literary scholars or historians, they can successfully serve as study courses for those who want to upgrade their qualifications. These skills are valuable in the labor market, where companies need employees to analyze and interpret large datasets. Familiarity with tools like Python, R, or data visualization software such as Tableau or Power BI can be crucial. The same can be said about project management and collaboration, which describe digital humanities, are also perceived as two crucial skills for managers.

Although the process of digitization requires skills to analyze big collections of data, equally important is the ability to employ qualitative methods in our understanding of the contemporary world. Considering that digital humanities focuses on contextualizing data with humanistic insights, it may help people make data-driven decisions based on cultural and social implications (Hayles, 2013). an increasingly valuable perspective in businesses seeking to combine data analysis with ethical and inclusive practices. As one of the advisers to the city of Helsinki, Finland, underlined during the World Economic Forum:

> To correct the asymmetries in power that currently define both the digital and non-digital realms, there are two routes we can take: we can tear down the already powerful, or we can lift up the currently disempowered. If we choose the route of empowerment, human-centric approaches and making data centre around people, and not the other way around, are essential in realising more fairness and equity in our societies (Bettinger, 2021).

In this perspective, people who understand both technological tools and their societal impacts can bridge the gap between technical and non-technical departments, creating a competitive edge for businesses. In addition to this, DH provides people with skills necessary for digital content creation, which is essential in marketing, public relations, and media industries. Understanding how to effectively communicate narratives through digital platforms (blogs, social media, podcasts) aligns with labor market demands for strong digital communication skills.

Another thing that should be taken into consideration while thinking about digital humanities and its impact on the future of work is curation of knowledge. Skills, such as the management of digital assets or the curation of digital collections, are among those that are more and more needed in the industry of the future. One must only think about the potential of digital humanities to train people how to preserve and manage large digital archives - not only in research projects but also in various industries, including media and governmental institutions. What is more, as there is a growing tendency for industries to rely on big

data, there is also a growing demand for individuals who understand not only how to manage data but how to preserve its historical context and ensure its ethical use.

Finally, digital humanities is invaluable when it comes to making the future of work more humane (Burdick et al., 2016). As ethical implications of technology are becoming critical in the fields, such as artificial intelligence, machine learning, and data privacy, DH may provide people with the set of skills that will allow them to focus not only on technology, but first and foremost, on people. According to the latest data, employees who can navigate the ethical challenges of emerging technologies are highly valuable in ensuring that tech development is socially responsible (Dhirani et al., 2023). Moreover, digital humanities contributes to making digital systems more accessible and equitable, which helps to understand how the process of digitization affects different groups of people. One must also remember about the potential of DH to develop soft skills, such as collaboration and communication. In addition to this, the analytical skills developed through digital humanities are transferable to problem-solving, decision-making, and innovation in the workplace, aligning well with the need for creative thinkers who can handle complex, real-world challenges.

This volume of studies proposes a new perspective on digital humanities. While DH has already established its place in contemporary humanities and social sciences, allowing scholars to use digital tools in their research projects, it still needs to gain position as a field supporting business and industry (Berry & Fagerjord, 2017). As such, digital humanities should be considered as an applied, and practical set of methods, techniques, and tools readily available for cooperative use not only by researchers or representatives of the GLAM industry, but for high-tech companies as well. The following definition combines major features of DH as an academic field and a framework for designing and teaching digital skills for the future of work:

Digital humanities is an interdisciplinary field, combining humanities and social sciences with computational methods and techniques, allowing scholars to analyze, preserve and disseminate their knowledge in innovative ways. DH integrates technical skills, e.g. data analysis, coding, digital content creation, with critical thinking and ethical insight. These features allow digital humanities to support the framework of the future of work and digital skills by equipping individuals with so-much needed skills, such as technological fluency, collaboration, data-driven decision-making and ability to keep the human factor at the center of the business and industry. As they more and more rely on digital tools and human-centered design, digital humanities fosters the development of adaptable, tech-savvy professionals capable of shaping and leading in the evolving digital economy.

Chapters in this volume of studies represent different disciplines and perspectives. Some of them focus on practical issues of the contemporary industry; some are more academia-oriented. However, they all fit into the triangle: digital humanities, digital skills, and the future of work. Such a wide range of topics and themes covered in the chapters is an example of an interdisciplinary approach to the global discussion on the hopes and fears that follow our understanding of the future workplace and skills. I am convinced that this volume of studies will contribute to the contemporary discourse on the future of work, expanding it into new directions. Moreover, the book represents opinions and research studies from various higher education institutions. Together, they form the European University EU4Dual, an alliance that focuses on dual studies and applied research. Several chapters are written by representatives of Ukrainian universities as a result of the 2024 Polish National Agency for Academic Exchange (NAWA) "Solidarity with Ukraine" program of cooperation between the Koszalin University of Technology and the Ivan Franko National University in Lviv, Vasyl Stefanyk Precarpathian National University in Ivano-Frankivsk, and the National Technical University of Ukraine - Igor Sikorsky Kyiv Polytechnic Institute.

References

Alliance of Digital Humanities Organizations. (n.d.). *About*. Digital Humanities Quarterly. https://digitalhumanities.org/dhq/about/about.html.

Berry, D. M., & Fagerjord, A. (2017). *Digital humanities: Knowledge and critique in a digital age*. Polity Press.

Bettinger, K. (2021, August 31). *12 ways a human-centric approach to data can improve the world*. World Economic Forum. https://www.weforum.org/agenda/2021/08/12-ways-a-human-centric-approach-to-data-can-improve-the-world/

Brennan C. Digital humanities, digital methods, digital history, and digital outputs: History writing and the digital revolution. *History Compass*. 2018; 16:e12492. https://doi.org/10.1111/hic3.12492.

Burdick, A., Drucker, J., Lunenfeld, P., Presner, T., Schnapp, J. (2016). Digital_ Humanities. United Kingdom: Penguin Random House LLC.

Carabregu-Vokshi, M., Ogruk-Maz, G., Yildirim, S. et al. 21st century digital skills of higher education students during Covid-19—is it possible to enhance digital skills of higher education students through E-Learning?. Educ Inf Technol 29, 103–137 (2024). https://doi.org/10.1007/s10639-023-12232-3

De Smet, A., Ellingrud, K., & Smit, S. (2023, January 23). What is the future of work? *McKinsey & Company*. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-future-of-work.

Dhirani LL, Mukhtiar N, Chowdhry BS, Newe T. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. *Sensors*. 2023; 23(3):1151. https://doi.org/10.3390/s23031151

Doumi, L., Goel, S., Kovács-Ondrejkovic, O., & Sadun, R. (2023, September). Reskilling in the age of AI. *Harvard Business Review*. https://hbr.org/2023/09/reskilling-in-the-age-of-ai.

European Commission. (2024). *Report on the state of the digital decade 2024*. Publications Office of the European Union. https://doi.org/10.2759/922

European Commission. (n.d.). *Social protection and inclusion: Key documents*. Retrieved September 23, 2024, from https://ec.europa.eu/social/main.jsp?catId=1606&langId=en.

Gold, M. K. (2012). *Debates in the Digital Humanities*. University of Minnesota Press.

Hayles, N. K. (2013). Comparative textual media: Transforming the humanities in the postprint era. In S. Schreibman, R. Siemens, & J. Unsworth (Eds.), *A companion to digital humanities* (pp. 431–443). Wiley. https://doi.org/10.1002/9781118680605.ch29

Jorgensen, T. (2019). Digital skills. Where universities matter. Learning & Teaching Paper (EUA).

Lang, G., & Triantoro, T. (2022). Upskilling and reskilling for the future of work: A typology of digital skills initiatives. Information Systems Education Journal, 20(4), 97–106.

Lynn, T., Rosati, P., Conway, E., van der Werff, L. (2023). Introducing the Future of Work: Key Trends, Concepts, Technologies and Avenues for Future Research. In: Lynn, T., Rosati, P., Conway, E., van der Werff, L. (eds) The Future of Work. Palgrave Studies in Digital Business & Enabling Technologies. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-31494-0_1.

McRae, E. R., Aykens, P., Lowmaster, K., & Shepp, J. (2024, January 11). *9 trends that will shape work in 2024 and beyond*. Harvard Business Review. https://hbr.org/2024/01/9-trends-that-will-shape-work-in-2024-and-beyond.

Rahaman, H. (2018). Digital heritage interpretation: a conceptual framework. *Digital Creativity*, *29*(2–3), 208–234. https://doi.org/10.1080/14626268.2018.1511602

Sanz, F. L. (2023, August 29). *Digital skills: A deep dive*. Digital Skills & Jobs Platform. https://digital-skills-jobs.europa.eu/en/latest/briefs/digital-skills-deep-dive.

Svensson, P. (2016). *Big digital humanities: Imagining a meeting place for the humanities and the digital*. University of Michigan Press. https://doi.org/10.3998/dh.13607060.0001.001

Talmage-Rostron, M. (n.d.). How will AI affect jobs? Nexford University. Retrieved November 7, 2024, from https://www.nexford.edu/insights/how-will-ai-affect-jobs.

Tapia, A. H. (2004), "The power of myth in the IT workplace: Creating a 24-hour workday during the dot-com bubble", *Information Technology & People*, Vol. 17 No. 3, pp. 303–326. https://doi.org/10.1108/09593840410554201.

van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2020). Determinants of 21st-Century Skills and 21st-Century Digital Skills for Workers: A Systematic Literature Review. Sage Open, 10(1). https://doi.org/10.1177/2158244019900176.

Andreas Baechler*, Liane Baechler**

Innovation Supporting inclusion: Utilising new technologies to create more accessible and diverse workplaces

Abstract: The modern world of work is undergoing unprecedented change. Rapid advances in technology and increasing digitalisation are changing the way we work, communicate with each other and perform our professional tasks. This article looks at the role of modern technologies in supporting inclusion and diversity in the world of work. In particular, it explores which new technological developments - from AI-driven systems to virtual and augmented reality (VR/AR) and advanced exoskeletons - can make workplaces more accessible for people with disabilities?

Keywords: new technologies, accessibility, workplace, future of work, people with disabilities

1. Introduction

The modern world of work is undergoing unprecedented change. Rapid advances in technology and increasing digitalisation are changing the way we work, communicate with each other and perform our professional tasks (Jacob, 2023). While this technological progress is opening up new horizons, one key challenge remains: How can technological change be used to make industrial workplaces more inclusive and accessible for all people?

The importance of inclusion in the workplace is not only a political, ethical or moral issue (United Nations, 2006), but also a key factor in the success of a company. Studies show that diverse teams are more innovative, creative and productive (SAP, 2023). However, one group is often overlooked that offers considerable potential: People with disabilities. In 2022, 27% of the EU population over the age of 16 lived with some form of disability. The proportion of people with disabilities in Germany is 30.3% and in Poland 24.2% (European Council, 2022). Many of them still have difficulties gaining access to the labour market. The integration of these people into the world of work is an opportunity that companies should not miss out on.

This article looks at the role of modern technologies in supporting inclusion and diversity in the world of work. In particular, it explores which new

* *Baden-Wuerttemberg Cooperative State University Campus Horb*
** *University of Cologne*

technological developments - from AI-driven systems to virtual and augmented reality (VR/AR) and advanced exoskeletons - can make workplaces more accessible for people with disabilities?

2. The changing workplace: Challenges and opportunities

The world of work has changed drastically in recent decades. The workplace used to be a physical place where tasks were carried out manually. Today, however, digitalisation enables a flexible and hybrid way of working where many tasks can be performed digitally. This has redefined the nature of work and forced organisations to adapt their work environments to keep pace with change (Oswald et al., 2022; Bächler, 2024).

For people with disabilities, this change has the potential to bring significant improvements (Aktion Mensch e.V., 2020; Bächler, 2020). For example, the digital transformation means that people who were previously excluded by physical barriers can now be better integrated. Through working from home or hybrid working models, people who are unable to work physically in an office can continue to contribute productively to the success of a company.

At the same time, challenges remain. Many digital work environments are not fully accessible and people with disabilities face barriers that prevent them from realising their full potential (Aktion Mensch e.V., 2020). This can be caused, for example, by the inaccessibility of software, inadequate ergonomic adaptations or a lack of training on how to use new technologies.

However, technological progress can overcome these challenges. Through customised technological solutions, companies can break down barriers and create an environment that supports all employees (Aktion Mensch e.V., 2020). However, this requires a deep understanding of the specific needs of employees and the willingness to invest in these technologies.

3. Types of disability and their limitations

The following chapter describes different types of disabilities and their specific limitations in order to provide a better understanding of the individual challenges and needs of people with disabilities in the working environment.

3.1 Physical disability

These disabilities affect physical mobility and motor skills. People with physical disabilities may have difficulty moving freely, carrying out everyday tasks or operating tools and machines.

- Restrictions:
  - Limited ability to walk (e.g. due to paraplegia, loss of limbs or muscle weakness)
  - Difficulty lifting, gripping or holding objects
  - Limited stamina or balance problems
  - Barriers in the physical environment (e.g. stairs, narrow doors)

3.2 Visual impairment

This type of disability affects vision and can range from mild impairment to complete blindness. People with visual impairments can have difficulty perceiving and processing visual information.

- Restrictions:
  - Blurred vision, tunnel vision, blindness
  - Difficulty reading, recognising faces or navigating in unfamiliar surroundings
  - Difficulties when working with visual displays or printed materials
  - Limited ability to recognise colours, shapes or contrasts

3.3 Hearing impairment

People with hearing impairments have problems hearing sounds or speech. This can range from mild hearing loss to complete deafness.

- Restrictions:
  - Difficulty understanding spoken language, especially in noisy environments
  - Inability to hear acoustic signals or alarms
  - Communication barriers in conversations or meetings without visual support such as sign language or subtitles
  - Difficulty making phone calls or following audio instructions

3.4 Mental disability

Cognitive impairments affect mental processes such as thinking, learning, remembering or problem solving. People with cognitive disabilities often have difficulty organising complex tasks or concentrating on a specific task.

- Restrictions:
  - Difficulties in processing information or learning new tasks
  - Memory problems, especially with complex or multi-step tasks
  - Problems with planning and organising tasks
  - Limited ability to react quickly to changes or stress

3.5 Psychological disabilities

Psychological disabilities refer to mental health problems that affect daily life and work. These include illnesses such as depression, anxiety disorders or bipolar disorder.

- Restrictions**:**
  - Difficulties regulating emotions or dealing with stress
  - Limited concentration and motivation
  - Problems with social interactions or coping with conflicts
  - Increased fatigue and reduced resilience

These types of disability lead to different challenges in everyday life and in the workplace, but require customised solutions and support (Rehadat, 2024; KOFA, 2024).

Psychological disabilities are not discussed in detail in the following work, as they present particular challenges due to their difficult to classify characteristics, the strong subjective and daily fluctuations, and because they can only be supported by technology to a limited extent so far.

4. Classification of technologies for accessibility in the workplace

The technologies that can be used to promote accessibility in the workplace can be divided into four main categories: No-Tech, Low-Tech, Mid-Tech and High-Tech (Wendt et al., 2011; Bächler et al., 2023; York et al., 2024).

Each category offers different solutions to support people with disabilities in the workplace, with technological advances ranging from simple adaptations to advanced, AI-powered systems.

4.1 No-tech solutions

No-tech solutions to promote accessibility in the workplace are often simple adaptations that do not require complex technology. They are usually based on organisational measures or physical adjustments to the working environment. One example is the provision of ramps or wheelchair-accessible workstations to make it easier for people with reduced mobility to access and use the workplace. Personal assistance can also be used to support people with disabilities in their day-to-day work, for example by helping them to navigate through the workplace or carry out specific tasks.

Another form of no-tech support is the customisation of work tasks. For example, people with cognitive impairments can be given tasks that are tailored to their

abilities so that they can work productively. These inclusion measures require a high degree of flexibility and adaptability on the part of the employer, but can often be implemented quickly and cost- effectively.

4.2 Low-tech solutions

Low-tech solutions refer to simple, easily accessible aids that generally do not require electricity or advanced technologies. An example of this are specially shaped tools or additional handles that enable people with limited fine motor skills to do their work more easily and efficiently. For people with visual impairments, simple visual aids such as enlarged documents or instructions in large print can be used.

These solutions are cost-effective and do not require extensive technical knowledge, making them a popular option for companies that want to take the first steps towards promoting inclusion. However, they often only provide support for specific tasks and do not cover all the needs that people with disabilities have.

4.3 Mid-tech solutions

Mid-tech solutions are more technologically advanced and require some customisation and implementation. They often include electronically supported devices that improve access to information or make physical work easier. One example is the height-adjustable workstation, which enables people with motor impairments to adapt their working environment ergonomically.

These technologies can also support complex tasks. Another example is specialised keyboards or speech recognition software that enables people with impaired fine motor skills to use computers more efficiently, as well as acoustic systems that amplify auditory signals and thus enable hearing-impaired people to access acoustic information. Although these technologies require an investment, they offer significant long-term benefits in terms of employee productivity and well-being.

4.4 High-tech solutions

High-tech solutions represent the cutting edge of technological innovation and provide advanced support for people with disabilities. Examples of these technologies include AI- powered exoskeletons that enable people with mobility impairments to walk again or perform complex physical tasks. These exoskeletons are often used in areas where physical labour is required, such as manufacturing or construction.

Another example is AR and VR systems that enable people with sensory or cognitive impairments to experience immersive learning and working environments.

These technologies can be used in employee training, for example, to learn new skills or simulate complex work processes (Inklusion 4.0, Gesellschaft für Bildung und Beruf e.V., 2024).

AI-assisted hearing aids and visual aids are further examples of high-tech solutions that significantly improve access to audiosensory and visual information.

The implementation of high-tech solutions often requires a significant investment in the technology itself as well as in training and support for employees. Nevertheless, they offer the potential to fundamentally change the world of work and permanently remove barriers.

5. Artificial intelligence in the world of work: a new dimension of inclusion

The integration of AI into the technologies described above offers a new dimension of inclusion for people with disabilities. With the ability to process large amounts of data and recognise patterns, AI can develop adaptive solutions that continuously and individually adapt to the needs of users to ensure maximum efficiency and inclusion (Steil et al., 2023; KI-Assist-Projekt, 2022).

5.1 AI and physical and motor impairments

AI-controlled exoskeletons can be a revolution for people with physical or motor impairments. These devices can support users' movements and thus significantly improve their mobility (Müller, 2023). For example, exoskeletons can be used in production to facilitate the lifting of heavy loads and reduce the risk of injury (Windhausen, 2022).

In addition, AI-supported robots can take on tasks that require precise movements, such as the assembly of small parts. This reduces physical strain and enables people with motor impairments to work productively in labour processes with high physical demands (Windhausen, 2021).

5.2 AI and visual impairments

People with visual impairments can be supported by AI-supported systems such as AR glasses that recognise objects in the environment and provide information via voice or tactile feedback in real time. These technologies, such as AR glasses that read out texts, describe colours or display obstacles, as well as apps such as Seeing AI that enable virtual vision, describe things in the smartphone camera's field of vision and make it easier to identify them (Meisel et al., 2024). This gives people with visual impairments greater autonomy in their day- to-day work.

The ongoing development of such technologies means that they are continuously improving and becoming smaller and lighter, such as the smart glasses from Rayban and Meta (Ray-Ban, 2024). AI systems learn from interactions with users and adapt to their specific needs, further increasing the comfort and effectiveness of these technologies.

5.3 AI and hearing impairments

AI also offers innovative solutions for people with hearing impairments. Modern hearing aids equipped with AI automatically adapt to different acoustic environments and filter out background noise to make speech signals easier to hear. These technologies enable people with hearing impairments to participate more effectively in conversations and meetings, making it easier for them to integrate into everyday working life (Weckbrodt, 2023).

AI-controlled AR glasses can also convert spoken language into text in real time so that people with hearing impairments can read spoken information directly on a screen (Karaboga, 2022). This technology has the potential to overcome communication barriers and enable people with hearing loss to participate more fully.

5.4 AI and cognitive impairments

People with cognitive impairments can be supported by AI-supported solutions in information processing and task organisation. AI-based cognitive assistants can support the user in planning and performing complex tasks by setting reminders, dividing tasks into manageable steps and providing real-time feedback. These systems are particularly valuable in work environments that require a high degree of organisation and concentration (Steil et al., 2023; AI-Assist project, 2022).

AI systems can also act as personal assistants (AI-Assist project, 2022), keeping an eye on important appointments and tasks and reminding the user to complete them.

6. Immersive training experiences through VR/AR technologies

One of the most interesting developments in the field of workplace integration is the use of virtual reality (VR) and augmented reality (AR) for training purposes. These technologies not only offer new learning opportunities, but also create a deeper understanding of the challenges faced by people with disabilities in the workplace (Fell, 2024).

Organisations can use VR systems to create immersive training experiences that enable all employees to better understand the perspectives of their colleagues

with disabilities. For example, such training can simulate what it is like to work with a visual or hearing impairment, raising awareness of the importance of accessibility and inclusion (Faster Capital, 2024).

7. Technologies in use for different types of disability

To illustrate the range of potential applications of new technologies, the following table 1 provides an overview of the different types of disabilities, categories of technological solutions and their possible applications in the world of work.

Table 1: Overview of technologies in use for different types of disability

Type of Disability	Category	Potential Areas of Application in the Workplace	Examples from the Work environment
Physical and Motor Impairments	No-Tech	Adapting the work environment	Personal assistance, consultation on workplace adaptation
	Low-Tech	Support for physical tasks	Platform, additional grips for tools, specially shaped tools
	Mid-Tech	Ergonomic adjustments, improved accessibility	Height-adjustable workstation, pick-by-light systems, specialised keyboards
	High-Tech	Extension of mobility and physical capabilities, maximum mobility, and integration into complex work processes	(AI-driven) exoskeletons, collaborative robots, (AI-supported) augmented reality glasses, electric wheelchairs, smart prostheses
Visual Impairments	No-Tech	Consultation and assistance	Adapted work tasks, personal assistance
	Low-Tech	Support for visual tasks	Large print instructions, document holders
	Mid-Tech	Enhancing visual perception and information processing	Electronic magnifiers, special displays, explanatory videos in simple language
	High-Tech	Extension of visual capabilities through technology, restoration, or enhancement of vision through innovative technologies	(AI-supported) AR glasses with camera system, implantable neurostimulators

Type of Disability	Category	Potential Areas of Application in the Workplace	Examples from the Work environment
Hearing Impairments	No-Tech	Consultation and communication support	Adapted work tasks, personal assistance
	Low-Tech	Support for communication	Large print, simple visual signals
	Mid-Tech	Enhancing auditory perception	Hearing amplifiers, voice-controlled machine operation
	High-Tech	Extension of auditory capabilities through technology, restoration, or enhancement of hearing through innovative technologies	(AI-supported) AR glasses with auditory signals, complex hearing systems, smart devices with audio support, implantable hearing devices
Cognitive Impairments	No-Tech	Support through adaptation of tasks and work environment	Adapted work tasks, personal assistance
	Low-Tech	Simplification of work processes	Structured work instructions, material provision
	Mid-Tech	Support through technological solutions for better information processing	Explanatory videos in simple language, smart devices with cognitive assistance functions
	High-Tech	Enhanced support through interactive and adaptive technologies, innovative solutions for full integration and support of complex tasks	AR/VR projection units, intelligent assistance systems, brain- computer interaction solutions, autonomous robots with cognitive assistance

8. Ethical considerations and challenges in the implementation of technologies

Although the technological developments are promising, there are also ethical considerations and challenges that need to be taken into account during implementation. These include issues of self-determination, data protection and the potential risks associated with the use of AI algorithms. For example, AI systems developed to support people with disabilities may also have unintended biases that penalise certain user groups.

Another problem is the possible dependence on technologies that could give people the feeling of having less control over their work. Organisations need to ensure that these technologies are implemented in a way that does not compromise employee autonomy but supports it (Feichtenbeiner et al., 2022).

9. Guidelines for the implementation of technology to promote inclusion

To realise the full benefits of new technologies to promote inclusion, a holistic approach is required. Organisations need to invest not only in technological solutions, but also in training and raising awareness among their employees. A successful approach combines technological innovation with a strong commitment to inclusion and acceptance in the corporate culture.

9.1 Holistic approach to implementation

Implementation should be a step-by-step process, starting with a thorough needs analysis to understand the specific requirements of employees. Suitable technological solutions can then be selected and integrated into the existing working environment. It is important that all employees are involved in the process and trained in the new technologies.

9.2 Organisational commitment

In addition to technological support, it is crucial that companies promote an inclusive corporate culture. This can be achieved through regular training, raising awareness of the needs of people with disabilities and promoting openness and acceptance. Only through a combination of technological advancement and cultural change can organisations create a truly inclusive working environment.

10. Conclusion and recommendations for companies

Promoting diversity and inclusion in the workplace requires a holistic approach that combines technological innovation with strong educational and organisational commitment.

Organisations should strategically implement proven technologies such as AI, AR, VR and advanced robotics systems to break down barriers and create a more accessible and diverse working environment. In doing so, it is essential to consider the specific needs of the workforce and place ethical considerations

and user empowerment at the centre. By integrating these technologies, not only can the productivity and well-being of employees be increased, but new, diverse perspectives can also be introduced into work processes.

Ultimately, the use of new technologies offers companies the opportunity to increase innovation and productivity and pave the way for an inclusive future. A holistic approach that combines technology with a strong commitment to inclusion is key to making workplaces more accessible and diverse and realising the full potential of the workforce

References

Aktion Mensch e.V. (2020). Digital participation of people with disabilities - trend study. Sinus Institute, Heidelberg/ Berlin.

Bächler, L. (2020). Participation in work through technical assistance [Dissertation]. University of Siegen, Siegen. https://doi.org/10.25819/ubsi/4284.

Bächler, L. (2024). Work(ing) with the help of digital assistive technology - consequences for workshops for people with disabilities. Living Together, 32(2), 106–113.

Bächler, L., Feichtinger, M., Huenermund, H., Krstoski, I. & Thiele, A. (2023). Hochschulnetzwerk Assistive Technologien: Hintergrund, Zielsetzungen und Positionen. Kongress der Gesellschaft für Unterstützte Kommunikation.

European Council (2022), Facts and figures on disability in the EU - Consilium (europa.eu).

Faster Capital (2024). Virtual reality for disability simulation: Inclusive Innovation: How VR can Transform Disability Awareness. Virtual reality for disability simulation: Inclusive Innovation: How VR Can Transform Disability Awareness - FasterCapital.

Feichtenbeiner, R., Stähler, L. & Beudt, S. (2022). Ethics, AI & human disability. Ethical Guidelines and Methodological Approaches for Inclusive Artificial Intelligence. Results report of the KI.ASSIST project. Federal Association of German Vocational Training Centres.

Fell, T. Artificial intelligence (AI), 3D technology and VR/AR revolutionise learning and development: A four-stage journey. Immersive Learning News. Artificial intelligence (AI), 3D technology and VR/AR are revolutionising learning and development: a four-stage journey - Immersive Learning News.

Inklusion 4.0, Gesellschaft für Bildung und Beruf e.V. (2024), Inklusion 4.0 - Ein Projekt der GBB e.V. (inklusion4punkt0.net).

Jacob, M. (2023). Digitalisation of the world of work. Springer Fachmedien Wiesbaden.

Karaboga M., Frei N., Ebbers F., Rovelli S., Friedewald M., Runge G. (2022): Automated recognition of voice, speech and face. Technical, legal and social challenges. In TA-SWISS Publication Series (ed.): TA 79/2022. Zurich: vdf.

KI.ASSIST project (2022). AI technologies and occupational participation of people with disabilities. Results and recommendations from the KI.ASSIST project. Federal Association of German Vocational Training Centres, AI technologies and vocational participation of people with disabilities (ki-assist.de).

Competence centre for securing skilled workers (2024). Federal Ministry of Economics and Climate Protection (BMWK) Berlin.

Meisel, P., Ronsdorf, J. (2024) AI & Inclusion: Developing technologies with and for people with disabilities. Microsoft News. AI & Inclusion: Developing technologies with and for people with disabilities | News Centre Microsoft.

Müller, G. (2023) Two steps back into life. Red Bull Vienna. Exoskeleton: Gregor Demblin can walk despite paralysis (redbull.com).

Oswald, G., Saueressig, T., Krcmar, H. (2022). Digital transformation. Springer Fachmedien Wiesbaden.

Ray-Ban, Meta (2024). Ray-Ban | Meta smart glasses 2024 | Ray-Ban® EN.

Rehadat (2024), Cologne Institute for Economic Research e.V.

Steil, J. J., Bullinger Hoffmann, A., André, E. et al.: Mit KI zu mehr Teilhabe in der Arbeitswelt.

Potentials, applications and challenges. Whitepaper from the Plattform Lernende Systeme, Munich. https://doi.org/10.48669/pls_2023-4.

SAP, 2023, Diversity in the workplace: The stats are in | SAP Insights.

United Nations (ed.). (2006). United Nations Convention on the Rights of Persons with Disabilities. https://www.un.org/disabilities/documents/convention/convention_accessible_pdf.pdf Weckbrodt, H. (2023). Dresden scientists work on implantable hearing aid. Oiger - News from business and research. Dresden scientists work on implantable hearing aid - Oiger.

Wendt, O. & Lloyd, L. L. (2011). Definitions, history, and legal aspects of assistive technology. In O. Wendt, R. W. Quist & L. L. Lloyd (Hrsg.), Augmentative and alternative communication perspectives: Bd. 4. Assistive technology: Principles and applications for communication disorders and special education (1st ed., S. 1–22). Emerald Group Pub.

Windhausen, E. (2021). An old profession and a modern aid: How a scissor fitter works with bionic support. Inclusive work. An old profession and a modern aid: How a scissor fitter works with bionic support - Inclusive working life (lwl.org).

Windhausen, E. (2022). Exoskeletons explained simply: Physical support at work and in everyday life.

Inclusive work. Exoskeletons explained simply: Physical support at work and in everyday life (with video) - Inclusive working life (lwl.org).

York, J., Bächler, L. & Jochmaring, J. (2024): Technology for the future of labour participation. *Journal of Inclusion, 19*(2), xx–xx. https://www.inklusion-online.net/index.php/inklusion- online/article/view/xxx.

Andrea Honal, Alexandra Advani, Dorothee Beez*

Virtual Reality vs. Face-to-Face: Assessing the Impact of Virtual Reality Public Speaking Training on Anxiety Reduction among Business Students – A Randomized Controlled Trial

Abstract: Effective communication is vital in higher education. For those studying business, mastering public speaking is key to their academic and career success. Yet, a significant number of these students express a fear of performing in front of an audience, commonly termed Public Speaking Anxiety (PSA). This randomized controlled trial assessed a Virtual Reality (VR)-based public speaking training's efficacy using a convenience sample of undergraduate business students. 67 students were divided into intervention (VR training with system feedback) and control group (traditional face-to-face presentations with expert feedback). PSA was evaluated pre- and post-intervention using the German version of the Self-Statements During Public Speaking (SSPS) scale. Both groups exhibited a reduction in PSA, but the VR group showed a significant decrease in all negative self-statements and displayed a preference for unbiased VR feedback. While the study's findings are promising, the limited sample size underscores the need for future research. VR has the potential to reduce PSA and enhance presentation skills. Rather than replacing traditional face-to-face training with instructor feedback, we aim to establish VR as an alternative. This approach not only offers potential time and resource savings but also aligns closely with the preferences of the millennial and Generation Z student populations.

Keywords: higher education, public speaking anxiety, virtual reality-exposure therapy, oral presentation skills, direct feedback, business students

Introduction

Oral presentation and public speaking skills are critical components of effective communication and are essential in management roles (Baccarani & Bonfanti, 2015). Many modules in business programs use presentations as a form of assessment and require students to verbally engage in small and large group settings to enhance learning (Moskal et al., 2008). For instance, Brink and Costigan (2015)

* *Baden-Wuerttemberg Cooperative State University (DHBW), Mannheim, Germany*

discovered that 76% of business curricula included a learning goal related to oral presentations. While the ability to present effectively in front of a large audience is perceived, today more than ever, as critical for young professionals' success in the workplace (Smith & Sodano, 2011; Van Ginkel et al., 2019), the majority of students start their careers with insufficient Oral Presentation Skills (OPS). Their education has failed to equip them with the skills needed to thrive in the work environment (Andrews & Higson, 2008; Brink & Costigan, 2015; Chan, 2011; Gibson & Sodeman, 2014; Gray, 2010; Jackson, 2010). Given the upsurge in Public Speaking Anxiety (PSA) within the student population (Hinojo-Lucena et al., 2020; Rodero & Larrea, 2022; Sarpourian et al., 2022) and the crisis-induced shift from on-campus to online or blended teaching formats, limiting opportunities for students to practice presentations in front of peers, it is plausible that the reduced chances for real-time audience exposure may contribute to an intensification of PSA. Therefore, analyzing PSA in the student population and developing solutions to counteract is key to overcoming the crisis-induced OPS gap.

Cognitive-Behavioral Therapy (CBT) has traditionally been used to treat PSA by exposing individuals to feared social situations (England et al., 2012; Reeves et al., 2022). Exposure therapy, an acknowledged method for treating anxiety disorders, is now being complemented by emerging VR therapies gaining traction among scholars (Harris et al., 2002; Hinojo-Lucena et al., 2020; Rodero & Larrea, 2022; Valmaggia et al., 2016). VR offers a unique avenue for exposure therapy, immersing students digitally in the very social situations they fear.

Virtual Reality Exposure Therapy (VRET) surpasses conventional CBT, offering technological advantages (Premkumar et al., 2022). Traditional methods may be limited when students struggle to vividly imagine scenarios or when creating controlled environments with suitable audiences and locations becomes challenging (Šalkevičius et al., 2019; Takac et al., 2019). However, VR technology holds promise for self-guided exposure therapy, allowing users to independently regulate their exposure to feared social situations without the need for an instructor (Premkumar et al., 2021). It preserves individual privacy, mitigating unpleasant public discomfort (Brundage & Hancock, 2015; Yuen et al., 2019). Its immersive nature encompasses both mental and physical involvement, often exceeding real-world experiences in terms of immersion level (Fetscherin & Lattemann, 2008). Notably, VR's realism significantly influences individual perceptions and behaviors (Schmid Mast et al., 2018; Takac et al., 2019). This efficacy has contributed to the widespread adoption of VRET in treating Public Speaking Anxiety (PSA) (Šalkevičius et al., 2019).

VRET can be delivered in various formats, with two primary approaches being self-guided and therapist-led sessions (Premkumar et al., 2021). Various advantages are associated with self-guided VRET, such as user autonomy, flexibility and

accessibility. However, in choosing an instructor-led VRET intervention for our public speaking training in an educational setting, several reasons guided our decision. Firstly, opting for an instructor-led approach ensured equal exposure for all students, minimizing variations in the intensity and duration of practice and fostering a standardized study environment. This control was essential to mitigate potential disparities in skill development that could arise in a self-guided format. Additionally, the complexity of the VR software used necessitated immediate technical support, a benefit provided by having an instructor present. This support facilitated participants in navigating the software, addressing technical issues, and optimizing their overall experience. Moreover, the presence of an instructor played a crucial role in maintaining consistent student engagement and motivation throughout the VR public speaking training. This personalized encouragement contributed to a more active and participatory learning experience. Furthermore, the real-time monitoring of participant distress, made possible by the instructor's presence, allowed for immediate support and intervention if any student experienced heightened anxiety or discomfort during the public speaking training. It is worth noting that the instructor-led approach facilitated a parallel study design, with half of the students practicing in front of an audience while the other half received the VR treatment. Both groups received identical theoretical input on effective presentation delivery, ensuring a comparable foundation for evaluating the impact of the VR intervention.

Despite the enthusiasm around VR for anxiety treatment (Anderson et al., 2016), only a limited number of studies have specifically concentrated on the student population with a particular emphasis on PSA (Hinojo-Lucena et al., 2020). Previous studies on VR applications in education have primarily focused on usability instead of learning outcomes (Radianti et al., 2020). However, our current research responds to Radianti et al.'s (2020) call by evaluating changes in students' PSA, OPS, and overall learning experience, emphasizing the assessment of VR application learning outcomes.

In shaping our research direction, we abided by three guiding principles: (1) the innovative teaching approach should reduce students' PSA; (2) it should be adaptable to educational settings, meaning it can be integrated into existing modules; and (3) in tune with the evolving preferences and demands of business students, predominantly from the Generation Z.

Generation Z's relationship with technology is not just profound but extends to actively creating and sharing digital content across diverse platforms (Hernandez-de-Menendez et al., 2020). Recognizing the tech-savvy nature of this generation, the immersive and engaging nature of VR aligns with their affinity for innovative learning experiences. Our approach recognizes Generation Z's status as digital

natives, born into a world where technology is seamlessly integrated into daily life. The adaptable nature of VR training allows for integration into busy schedules while providing a novel and effective means of public speaking skill development. This adaptability is crucial as Generation Z, always connected and fast-paced in their activities, appreciates learning experiences that can be seamlessly woven into their routine (Hernandez-de-Menendez et al., 2020). By embracing the technological advancements (e.g. gamification) preferred by these generations (Saxena & Mishra, 2021), we aimed to enhance the overall appeal and effectiveness of the training, making it more attuned to the ways in which they engage with and absorb information.

With a twofold aim of reducing PSA and enhancing OPS, this study employs an intervention design as part of the module "Introduction to Research Methods and Academic Writing" for undergraduate business students, this study examines the value of VR applications in a real educational context and addresses the question of how VR-based public speaking training can be integrated into curricula to provide new, personalized opportunities to improve students' OPS. Previous studies have been constrained by their limited consideration of sub-criteria, overlooking crucial elements of oral presentation skills. Student participants will rehearse presentations before a virtual audience with varying demographics, characteristics, attention or difficulty levels, and audience sizes, while training activities are measured and visualized using trend analyses and statistics. The integration of Artificial Intelligence (AI) enhances user performance by regulating audience reactions and delivering immediate real-time feedback. This will strengthen students' OPS because they will instantly receive feedback about volume, eye contact, body language, gestures, fillers, and further relevant indicators to improve their presentation skills on the fly. By incorporating the previously mentioned subcriteria, beyond eye contact and speech rate, this study addressed the concerns raised by Van Ginkel et al. (2020), thereby enhancing the validity of the study.

This study aims to explore whether a brief public speaking training in front of a virtual audience with real-time AI-based feedback improves PSA in undergraduate business students. The overall research aim was to explore whether the VR Speech Training is more effective in terms of PSA reduction than a face-to-face presentation with instructor feedback.

In pursuit of this goal, two research objectives were formulated based on gaps identified in the literature mentioned above:

1. to explore the differential impact of VR versus on-campus public speaking training on students' PSA.
2. to investigate the extent to which students perceive such innovative tools as valuable for improving their presentation skills.

Public Speaking Anxiety and Higher Education

Oral presentations are one of the most widely used forms of assessment in higher education (Brink & Costigan, 2015; Moskal et al., 2008). Whether it is in front of a class, an audience of peers, or a panel of judges, presenting in front of others can be challenging, especially for students who face PSA (Valls-Ratés et al., 2022). Widely varying definitions of PSA have emerged since early research on "stage fright" (Lomas, 1937), mainly due to researchers' preferences for a particular word or phrase reflecting their theoretical stance (Bodie, 2010). In broad terms, PSA can be described as a form of social anxiety, where an individual fears performing in front of an audience. This type of socially based anxiety is associated with being apprehensive before presenting in front of an audience, resulting in disrupted communication (e.g. pauses, stuttering), and negatively affects social, academic, and career opportunities (Choi et al., 2015; Sarpourian et al., 2022). Also called glossophobia, PSA is further associated with various physiological changes, such as elevated heart and breathing rates (Tse, 2012). Instances of PSA have become prevalent among students, especially when they are aware that their performance is being evaluated (Grieve et al., 2021). Today, more than ever, student activities and assessments require social interactions, such as oral exams, job interviews, and class presentations (Brink & Costigan, 2015; Moskal et al., 2008). Thus, students who aim to thrive in their future careers should improve their OPS.

As defined within presentation research, oral presentation skills can be described as "a combination of knowledge, skills, and attitudes needed to speak in public to inform, self-express, relate, or to persuade" (De Grez, 2009, p. 5). Consequently, students' OPS can be enhanced by any or all of these aspects, referring to cognition, behavior, and attitude toward presenting (Van Ginkel et al., 2015). Since this study focuses in particular on VR as an innovative technology to improve students' oral presentation skills, it focuses solely on the presentation behavior aspect.

A potential solution to alleviate PSA and address speech delivery issues is to provide students with increased rehearsal opportunities for their oral presentations (Smith & Frymier, 2006; Valls-Ratés et al., 2022; Van Ginkel et al., 2019). Importantly, research indicates that practicing oral presentations in front of an audience is more effective than rehearsing alone (Menzel & Carrell, 1994) and therefore is key to students' speaking success and reducing PSA. However, the shift to online or hybrid learning models during the COVID-19 pandemic (Petronzi & Petronzi, 2020) has constrained students' chances of overcoming PSA through real-world practice. While traditional face-to-face rehearsals have proven

beneficial, the need for innovative solutions that address the current educational challenges has never been more pressing.

There is evidence that VR reduces levels of PSA (Lim et al., 2023; Reeves et al., 2022) and enhances students' OPS (e.g. Chollet et al., 2015). Compared to a face-to-face presentation with instructor feedback, Van Ginkel et al. (2019) even revealed that students' OPS could be significantly increased using VR. An argument for this finding relates to the fact that students highly appreciated the feedback they received after their presentation in virtual reality, due to its detailed and analytical character (Van Ginkel et al., 2020). In the current educational landscape, VR not only provides a safe and controlled environment for students to improve their public speaking skills without the constraints of physical barriers but also aligns with the tech-savvy demands and preferences of today's student population (Palmas et al., 2022).

Fusing Virtual Reality and Exposure Therapy

The most empirically supported and effective type of psychological intervention to treat social anxiety is CBT (Heimberg, 2002; Heimberg et al., 1993; Rodebaugh et al., 2004). In treating PSA, individual and/or group CBT has proven itself to be highly effective (Ponniah & Hollon, 2008; Powers et al., 2008). While exposure therapy is the most commonly used technique to treat social phobia, allowing individuals to gradually experience feared social situations, it can also be time and budget-consuming due to difficulty in finding suitable locations and audiences (Carl et al., 2019; Takac et al., 2019; Wallach et al., 2009). To overcome the limitations regarding traditionally delivered CBT, a more recent approach utilizes VR to immerse individuals into three-dimensional and simulated PSA scenarios, allowing them to experience a "real-life" scenario (Sarpourian et al., 2022; Takac et al., 2019). Compared to traditional face-to-face CBT interventions with in vivo exposure to treat PSA, several meta-analysis findings have indicated that VRET can be equally effective (Carl et al., 2019; Chesham et al., 2018; Fodor et al., 2018; Lim et al., 2023; Reeves et al., 2022). Consequently, research has started to emerge on the integration of VR into therapy, both for enhancing OPS (Batrinca et al., 2013; Palmas et al., 2019; Poeschl, 2017; Van Ginkel et al., 2020) and for addressing PSA (Anderson et al., 2005; Harris et al., 2002; Rodero & Larrea, 2022; Sarpourian et al., 2022; Takac et al., 2019; Wallach et al., 2009).

By using VR tools to treat PSA, individuals can experience the feared social situation in a safe environment, and by being repeatedly immersed in the simulated scenarios, speaking success will be increased (Denizci Nazligul et al., 2019).

VRET provides consistent and predictable scenarios, allows customization, and can be applied independent of location and audience through a head-mounted display. Paired with VR's potential to innovate higher education (Fabris et al., 2019; Greenwald et al., 2017), VRET might be a promising approach to overcome major limitations preventing the integration of presentation training into the curriculum. By fusing OPS training and VR, students can improve important factors, such as maintaining eye contact and reducing pauses in speech (Wörtwein et al., 2015). Furthermore, VR improves students' learning experience (McGovern et al., 2019), and learning outcomes (Fabris et al., 2019), enhances situated learning (Greenwald et al., 2017), and delivers detailed, individualized feedback (Van Ginkel et al., 2019) to students resource-effectively (e.g. reduced space requirements, multiple user interaction, flexibility, and scalability) (Carl et al., 2019; Takac et al., 2019; Wallach et al., 2009).

Feedback in VR and Public Speaking Performance

While feedback is considered being a crucial component of the learning process (Attali & van der Kleij, 2017; Hattie & Timperley, 2007; Shute, 2008), research examining the role of new technologies in developing unbiased and detailed feedback remains scarce (Merchant et al., 2014). However, some researchers suggest that using innovative technologies like VR can enhance students' competencies (Belboukhaddaoui & Van Ginkel, 2019; Van Ginkel et al., 2019; Van Ginkel et al., 2020). This is because interactive digital learning environments can simulate real-life processes and make it easier to provide feedback (Merchant et al., 2014).

From a scientific standpoint, it is uncertain whether a VR-based presentation task that provides feedback is as efficient as a face-to-face presentation task with feedback from an expert (Merchant et al., 2014; Van Ginkel et al., 2019). However, regarding the educational practice perspective, the present research focus is crucial because VR could assist in creating more efficient and effective learning environments by overcoming obstacles such as decreasing opportunities for teacher-student interactions and instructional time (Van Ginkel et al., 2015). Notably, the VR Speech Trainer enjoys greater acceptance, particularly from participants who do not experience public speaking anxiety (Palmas et al., 2021). Therefore, VR has the potential to address the challenges facing higher education curricula in the future, as it is more efficient in terms of reducing time and costs. Furthermore, it can provide "individualized" education, including personalized feedback, to a large number of students (Van Ginkel et al., 2019).

Methodology

Design

A randomized controlled trial compared commercially available public speaking training delivered through Virtual Reality (VR Speech Trainer) with a non-virtual counterpart involving instructor feedback. The study encompassed two treatment sessions for each participant.

Research Setting

In this study, we utilized a virtual audience through the VR Speech Trainer, a software developed by the EdTech company straightlabs GmbH & Co., for public speaking training. The objective was to investigate whether a brief public speaking session in front of this virtual audience, coupled with real-time AI-based feedback, effectively enhances PSA among undergraduate business students. The VR Speech Trainer was integrated into the module "Introduction to Research Methods & Academic Writing" at the Baden-Wuerttemberg Cooperative State University (DHBW) in Mannheim, Germany, using a convenience sample of undergraduate business students. The software VR Speech Trainer was used as the environment as it (1) represents a real-life (work) setting; (2) is responsive to the student's performance; (3) is capable of providing immediate feedback which directly has an impact on students' learning outcomes; (4) can be used at various difficulty levels.

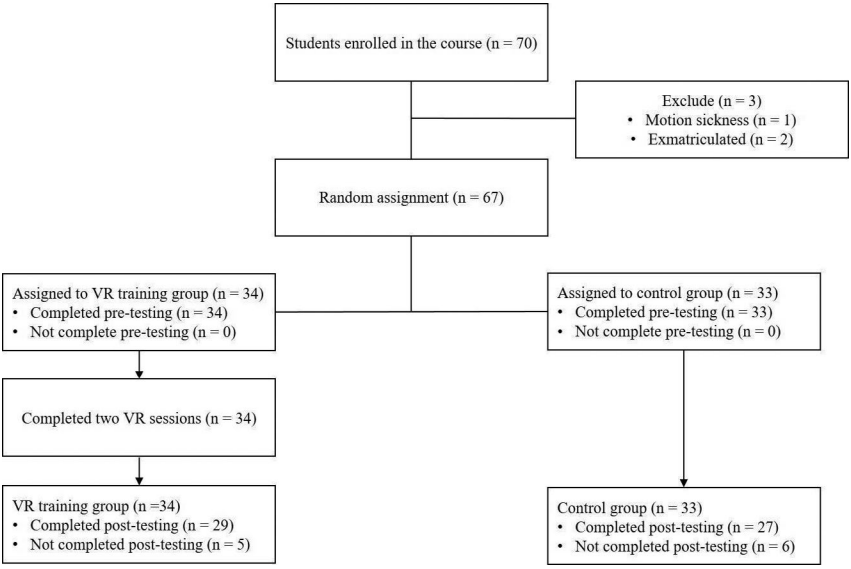
We assessed students' anxiety regarding public speaking through the utilization of a self-assessment questionnaire. Subsequently, we provide a detailed description of the study protocol:

1. Intervention group (virtual audience): In the virtual audience setting, participants receive instantaneous feedback as the audience responds in real-time. Positive behaviours, such as nodding and leaning forward, are indicators of an effective performance, while negative cues, like looking away or shaking heads, signify areas for improvement. Additionally, color-coded indications promptly signal when the speaker is losing the attention of the audience, enhancing the immediacy and specificity of the feedback loop.
2. Control condition (non-virtual, peer audience): In the control condition with a non-virtual, peer audience, participants receive feedback from the instructor following their presentation. Notably, no feedback is provided during the presentation itself, distinguishing this condition from the real-time feedback mechanisms employed in the intervention group.

Both conditions received two sessions of training, with one presentation in each session lasting for a total of 5–10 minutes. After the second presentation, all participants were asked to complete a self-assessment questionnaire, which took between 10–20 minutes.

To assess the efficacy of VR-based public speaking training against traditional on-campus training (which involves face-to-face presentations in a classroom setting with instructor feedback), we randomly assigned students to either the intervention or control group and subsequently secured informed consent from all participants.

Fig. 1: Selection of sample included in the final analysis



In total, 67 business students were assigned either to the intervention or control group (Fig. 1). Both the intervention and the control group were administered two online questionnaires, one at baseline and one post-intervention (after the two treatments). Students in the intervention group received two sessions of individual treatment, using a simulated meeting room scene (using the VR Speech Trainer software developed by straightlabs GmbH & Co. KG) and a head-mounted display with eye-tracking (Pico Neo 3 Pro-Eye). Each session of exposure lasted 5–10 min. The VR Speech Trainer allows the instructor to easily simulate different types of audience reactions (e.g. bored or enthusiastic), providing implicit feedback (Fig. 3) regarding the quality of a presentation

delivered by a student. For the VR sessions, the students had to deliver two impromptu presentations with two varying topics. These slides were uploaded to the VR Speech Trainer and were integrated into the VR scenario to ensure standardized conditions for each student. However, the content of the presentation was not a determining factor and was not assessed by the software; instead, the focus was on the delivery of the presentation. In the control condition, students participated in a similar training without the use of VR. Instead of utilizing the simulated meeting room scene and audience reaction simulation in a virtual environment, they delivered impromptu presentations in a traditional setting in front of their peers and received feedback from the lecturer afterwards. This non-VR condition provided a comparison to assess the impact of the virtual reality elements present in the intervention group, focusing on the differences between training with and without VR technology.

Fig. 2: Student perspective on immediate feedback in the VR Speech Trainer meeting room scene (source: straightlabs GmbH & Co. KG)

Procedure

The research procedure included the following steps:

1. All participants were provided with an impromptu speech in the form of an 11-slide presentation deck (one introduction slide followed by 10 slides of presentation material) with brand logos, entitled "Social media or not—justify

your answer" for the first treatment and "Luxury brand or not—justify your answer" for the second treatment. This was necessary to allow all participants to work from the same script and connect with a topic relevant to them.
2. Before performing their virtual presentations, participants were shortly introduced to the hardware and software. Students were provided with the Pico Neo 3 Pro Eye headset (already equipped with the VR Speech Trainer software) and required to put on the headset and navigate into the virtual classroom to deliver their first presentation.
3. When participants finished their presentation, the data collected by the VR Speech Trainer was presented to each participant individually using a screen display to discuss their presentation based on the dashboard results at the end.
4. This was the first time that participants were informed about the metrics measured by the VR Speech Trainer, namely time management, transcript, fillers, commonly used words, eye contact, volume, pace, body language, viewing direction, gestures, attention, and self-confidence. For a comprehensive technical breakdown of how this metrics are assessed, please refer to Palmas et al. (2021).

Measures

The SSPS scale is a 10-item questionnaire consisting of two 5-item subscales, the Positive Self-Statements (SSPS-P) and the Negative Self-Statements subscale (SSPS-N). The SSPS questionnaire is commonly used to estimate public speaking anxiety and has good psychometric properties (Hofmann & DiBartolo, 2000). In both student and clinical samples, the measure's 2-factor structure was confirmed, with internal consistency for SSPS-P ranging from .75 to .84 and SSPS-N from .83 to .86 in undergraduate cohorts, and similar results noted in clinical groups (Hofmann & DiBartolo, 2000). While there are other measures of public speaking anxiety available, the SSPS measures an aspect of public speaking anxiety that is separate from overall social anxiety, making it a targeted and specialized measure for this particular domain.

Statistical Analysis

Data were analyzed using SPSS for Windows, version 27.0. Participants' demographic characteristics were assessed using descriptive statistics (frequency, percentage, mean, and standard deviation [SD]). Within the intervention and control groups, the paired one-sided sample t-test was employed to compare PSA means before and after the intervention.

Results

Sample Description

Participants were randomly allocated to either the intervention or control group. The intervention group had an average age of 20.53 years (SD = 2.474) and the control group, had 20.11 years (SD = 1.968). Parity distribution was balanced between both groups, as detailed in Table 1.

Table 1: Mean age and parity distribution (%) for the intervention and control groups

Condition	N	Mean age ± SD [years]	Gender	
			Female	Male
Intervention group	29	20.53 ± 2.474	53.33 %	46.67 %
Control group	27	20.11 ± 1.968	59.26 %	40.74 %

Students' Progress in Overcoming Fear of Public Speaking

To evaluate students' levels of PSA, paired-sample t-tests were conducted for both the intervention and control groups. The results from the one-sided paired sample t-test are presented in Table 2.

Table 2: SSPS pre-and post-test scores for the intervention and control groups

Statements		Intervention (N = 29)			Control (N = 27)		
		Mean	SD	p	Mean	SD	p
1. What do I have to lose it's worth a try	Pre	3.41	1.181	.194	2.81	1.039	.365
	Post	3.66	.857		2.74	1.163	
2. I'm a loser	Pre	3.79	1.048	<.001**	4.07	1.035	<.001**
	Post	2.21	1.048		3.22	1.086	
3. This is an awkward situation but I can handle it	Pre	3.10	1.113	.315	2.63	.926	.230
	Post	3.24	.988		2.48	.849	
4. A failure in this situation would be more proof of my incapacity	Pre	3.66	1.344	<.001**	3.81	1.111	<.001**
	Post	2.55	1.152		2.48	.975	
5. Even if things don't go well, it's no catastrophe	Pre	3.17	1.136	.172	3.15	1.350	.253
	Post	3.48	.986		3.00	1.000	

Statements		Intervention (N = 29)			Control (N = 27)		
		Mean	SD	p	Mean	SD	p
6. I can handle everything	Pre	2.93	.961	.324	3.19	1.001	.300
	Post	2.83	1.002		3.30	.993	
7. What I say will probably sound stupid	Pre	3.76	1.023	<.001*	4.11	.892	.013
	Post	2.59	1.018		3.67	1.144	
8. I'll probably ‚bomb out' anyway	Pre	4.03	.865	<.001**	4.15	.907	.062
	Post	2.31	1.105		3.78	1.121	
9. Instead of worrying I could concentrate on what I want to say	Pre	4.24	.739	.156	2.22	.801	<.001**
	Post	4.03	.731		3.78	.801	
10. I feel awkward and dumb; they're bound to notice	Pre	3.72	1.162	.002*	3.70	1.171	.122
	Post	2.72	1.099		3.44	1.086	

Note. Items 1,3,5,6, and 9 comprise the "Positive Self-Statements" (SSPS-P), and items 2,4,7,8, and 10 the "Negative Self-Statements" (SSPS-N).
*p < .005
**p < .001

As can be observed in Table 2, working students who took part in the intervention programme aimed at examining the efficacy of VR-delivered public speaking training have benefitted from the brief treatment. Students in the intervention group showed decrease from pre-testing to post-testing in all negative statements "I'm a loser" (p <.001), "A failure in this situation would be more proof of my incapacity" (p <.001), "What I say will probably sound stupid" (p <.001), "I'll probably 'bomb out' anyway" (p <.001) and "I feel awkward and dumb; they're bound to notice" (p = .002).

Although the control group experienced decreases in negative statements such as "I'm a loser" (p < .001), "A failure in this situation would be more proof of my incapacity" (p <.001), and "What I say will probably sound stupid" (p <.013), it is important to highlight that the intervention group exhibited a significantly stronger effect with regard to the seventh statement, "What I say will probably sound stupid", which was ten times lower for students in the control group. Only the intervention group demonstrated a decrease for the eighth statement, "I'll probably 'bomb out' anyway", and the tenth statement, "I feel awkward and dumb; they're bound to notice", when compared to the control group.

In our evaluation, we did not consider the ninth statement of the SSPS questionnaire, which pertains to the ability to concentrate on what one wants to say instead of worrying. This omission is justified by the nature of our intervention, which involves impromptu speaking tasks where students are expected to deliver spontaneous presentations based on a short prompt. In such scenarios, students were unable to prepare their presentations in advance, and the topic itself was unknown to them.

Students' Perceptions of VR as an Enhancing Tool for OPS

To investigate the extent to which students perceive such innovative tools as valuable for improving their oral presentation skills, students completed the following self-statements on a 5-point Likert scale (Table 3).

Table 3: Descriptive statistics of students' perceptions regarding VR

Statements	Mean	SD	Median
I would endorse the use of VR in lectures.	3.76	0.83	4
VR helped me to know more precisely, what is important when presenting.	3.83	0.97	4
The usage of VR increased my motivation for my studies.	2.48	1.24	3

Students overall recognized the value of the VR intervention in their academic journey. The majority expressed a keen interest in using VR technology across various lecture formats, suggesting its potential as a universally practical tool in academic settings. An average score close to 4.00 on the statement, "I would endorse the use of VR in lectures" underscores this viewpoint. Furthermore, the data revealed that VR has significantly aided students in identifying the crucial aspects of effective presentations. This is evidenced by the average score of 3.83 for the statement, "VR helped me to know more precisely, what is important when presenting", indicating that VR has enabled students to focus on key presentation elements such as volume, body language, and eye contact. This immersive experience thus provided clarity on vital presentation aspects.

However, the enthusiasm for VR's integration into lectures and its perceived benefit in presentation clarity does not necessarily translate to an overall increased motivation for studies. The mixed response, indicated by an average score of 2.48 for the statement, "The usage of VR increased my motivation for my studies" suggests that while VR is a promising tool for specific tasks like presentations, its

impact on holistic academic motivation remains more nuanced. It is essential to recognize that the multifaceted nature of academic endeavors goes beyond just the act of presenting.

Building on the positive feedback from the intervention group, participants from the control group were also offered an opportunity to undergo VR presentation training after the study's conclusion.

Discussion and Limitations

The adoption of VR technology to address challenging presentation scenarios in a safe environment with a virtual audience and real-time AI feedback shows promising results. The VR setting provides an easily replicable training environment, eliminating the logistics of organizing a physical audience for simulating training situations each time.

The objectivity of AI provides a consistent evaluation metric. This consistency contrasts with traditional methods, which might provide fleeting, generalized feedback without in-depth analysis. Even when comprehensive feedback is provided in traditional settings, nuances like eye contact, attention span, or filler words, which the VR software assesses, might be overlooked. Another concern with conventional training lies in feedback variability. Feedback may range from being constructive and insightful to being subjective and inconsistent, making it challenging for students to discern its relevance. This inconsistency hinders a concrete evaluation of traditional presentation training's effectiveness.

However, one significant limitation of our study pertains to the observed decline in PSA within the control group. This decrease might be attributable to the study's limited sample size and the value of verbal instructor feedback. While it is plausible that the provision of high-quality feedback from the instructor might have reduced students' PSA levels in the control group; the data underscores the VR Speech Trainer's potential in significantly reducing PSA.

Another potential limitation is the brief duration of our intervention. With only two sessions, each lasting between 5–10 minutes, questions arise concerning the long-term effectiveness of the VR approach. While our study showed promise in the short term, it remains uncertain how sustained or more extended VR interventions might impact participants. Would the effects be more profound, or would they level off after a certain point? This study's design does not offer conclusive answers to these questions.

Moreover, our research was conducted in a specific context with a distinct set of participants. Thus, the findings might not be generalizable to broader populations

or different settings. Different groups might respond differently to VR interventions, and our study did not capture this variability.

Lastly, while our study highlighted the benefits of VR-based public speaking training, it is essential to recognize that it does not seek to replace traditional public speaking training or undervalue the importance of human feedback. We propose VR as a complementary method. Though we noted benefits in using VR, traditional methods, backed by years of pedagogical practice, have their own set of advantages that our study did not extensively explore.

Conclusions and Future Works

Our findings support that VR-based public speaking training can be a valuable alternative to traditional face-to-face presentations with instructor feedback for reducing PSA, providing both unbiased feedback in a safe environment and advantages concerning time and resource costs. The obtained data demonstrate that while both VR and traditional training reduced PSA levels among business students, the VR training resulted in a highly significant difference between the pre-intervention and post-intervention responses for all negative self-statements of the SSPS scale. When these results are considered in the context of the difference in time to prepare a face-to-face session with location, audience and instructors, these strongly favor VR, suggesting that VR should be included as an alternative to traditional public speaking training in business modules.

Despite the enthusiasm around VR for anxiety treatment (Anderson, Edwards & Goodnight, 2016), only a limited number of studies have specifically concentrated on the student population with a particular emphasis on PSA (Hinojo-Lucena et al., 2020). Previous studies on VR applications in education have primarily focused on usability instead of learning outcomes (Radianti et al., 2020). The results obtained in this study are consistent with previous research, emphasizing that VR training and exposure can effectively reduce PSA in students (see Hinojo-Lucena et al., 2020 for a review) and enhance confidence when engaging in discussions or meetings (Palmas et al., 2019; Slater et al., 2020). However, the main strengths of the current work are the use of sub-criteria beyond eye contact and speech rate, the focus on learning outcomes rather than usability, and the randomized study design. By incorporating the previously mentioned sub-criteria, beyond eye contact and speech rate, this study addressed the concerns raised by Van Ginkel et al. (2020).

While the benefits of incorporating gamification elements into VR-based public speaking training, as highlighted by Palmas et al. (2022), are apparent,

it would be imperative for future research to delve deeper into this aspect. We recommend tapping into the broaden-and-build theory of positive emotions, suggesting that positive emotions can broaden individuals' momentary thought-action repertoires and build their enduring personal resources (Fredrickson, 2001). In the context of VR, the enjoyment derived from gamification might foster positive emotions, shifting the perception of presenting from a source of negative emotions to one associated with pleasure. This transformative experience might not only create pleasurable associations with presenting but also significantly aid in overcoming PSA by potentially reducing the impact of negative emotions (Cohen & Huppert, 2018). Through this, students might be more inclined and equipped to build and refine their presentation skills in a supportive environment.

In conclusion, the results of this randomized controlled trial provide evidence that VR-based public speaking training is effective in reducing PSA levels among business students. Based on these findings, we recommend the adoption of VR training as an alternative method for enhancing presentation skills for several reasons. Firstly, it offers objectivity in evaluation, providing a standardized and consistent assessment of performance. Additionally, it provides a safe and controlled environment for learners to practice without the pressure and judgement they may experience in real-life situations. With VR, students can develop their presentation skills in a safe and controlled environment. They can simulate and confront situations that may be stressful (e.g. fear of embarrassment or making mistakes) in the real world. Students can also benefit from independence, as they can engage in VR training at their own pace and convenience, without being constrained by group dynamics or time limitations. Furthermore, VR training allows for repeated practice of presentations until learners gain confidence in real-world scenarios without incurring additional costs or logistical challenges. VR enables the customization of training to meet the needs and goals of each student. Different scenarios and difficulty levels can be easily adjusted to provide an optimal challenge for learners. The inclusion of gamification elements adds an element of fun and engagement to the training experience. Through interactive experiences, students become more involved in the training and can benefit more from the learning content. The immediate and unbiased feedback provided during live VR sessions, as well as the detailed analysis post-presentation, enhance the learning process. By engaging in VR public speaking training, students have the opportunity to overcome their fears before encountering similar situations in real-life professional settings. Given the results of this paper, we believe efforts to integrate VR-based public speaking training in business programs will be valuable for both lecturers and students.

Data Availability

The data that support the findings of this study were obtained from student participants of the Baden-Wuerttemberg Cooperative State University (DHBW). Due to privacy concerns and institutional guidelines, the raw data are not publicly available. However, the data can be made available from the authors upon reasonable request and with the appropriate permissions from the Baden-Wuerttemberg Cooperative State University (DHBW).

Correspondence to: Alexandra Advani
https://orcid.org/0009-0004-7441-8837
Alexandra.Advani@dhbw-mannheim.de

Conflict of interest

The authors declare no conflict of interest (financial or otherwise) related to the work submitted for publication.

References

Anderson, P. L., Edwards, S. M., & Goodnight, J. R. (2016). Virtual Reality and Exposure Group Therapy for Social Anxiety Disorder: Results from a 4–6 Year Follow-Up. *Cognitive Therapy and Research*, *41*(2), 230–236. https://doi.org/10.1007/s10608-016-9820-y.

Anderson, P. L., Zimand, E., Hodges, L. F., & Rothbaum, B. O. (2005). Cognitive behavioral therapy for public-speaking anxiety using virtual reality for exposure. *Depression and Anxiety*, *22*(3), 156–158. https://doi.org/10.1002/da.20090.

Andrews, J., & Higson, H. (2008). Graduate employability, 'soft skills' versus 'hard' business knowledge: A European study. *Higher Education in Europe*, *33*(4), 411–422.

Attali, Y., & van der Kleij, F. (2017). Effects of feedback elaboration and feedback timing during computer-based practice in mathematics problem solving. *Computers & Education*, *110*, 154–169.

Baccarani, C., & Bonfanti, A. (2015). Effective public speaking: A conceptual framework in the corporate-communication field. *Corporate Communications: An International Journal*, *20*(3), 375–390.

Batrinca, L., Stratou, G., Shapiro, A., Morency, L.-P., & Scherer, S. (2013). Cicero - Towards a multimodal virtual audience platform for public speaking training. In R. Aylett, B. Krenn, C. Pelachaud, & H. Shimodaira (Eds.),

Intelligent virtual agents (IVA 2013) (Lecture Notes in Computer Science, Vol. 8108). Springer. https://doi.org/10.1007/978-3-642-40415-3_10.

Belboukhaddaoui, I., & Van Ginkel, S. (2019). Fostering oral presentation skills by the timing of feedback: An exploratory study in virtual reality. *Research on Education and Media*, *11*(1), 25–31. https://doi.org/10.2478/rem-2019-0005.

Bodie, G. D. (2010). A racing heart, rattling knees, and ruminative thoughts: defining, explaining, and treating public speaking anxiety. *Communication Education*, *59*(1), 70–105. https://doi.org/10.1080/03634520903443849.

Brink, K. E., & Costigan, R. D. (2015). Oral communication skills: Are the priorities of the workplace and AACSB-accredited business programs aligned? *Academy of Management Learning & Education*, *14*(2), 205–221.

Brundage, S. B., & Hancock, A. B. (2015). Real enough: using virtual public speaking environments to evoke feelings and behaviors targeted in stuttering assessment and treatment. *American Journal of Speech-Language Pathology*, *24*(2), 139–149. https://doi.org/10.1044/2014_ajslp-14-0087.

Carl, E., Stein, A. T., Levihn-Coon, A., Pogue, J. R., Rothbaum, B., Emmelkamp, P., Asmundson, G. J., Carlbring, P., & Powers, M. B. (2019). Virtual reality exposure therapy for anxiety and related disorders: A meta-analysis of randomized controlled trials. *Journal of Anxiety Disorders*, *61*, 27–36.

Chan, V. (2011). Teaching Oral Communication in Undergraduate Science: Are We Doing Enough and Doing it Right? *Journal of Learning Design*, *4*, 71–79.

Chesham, R. K., Malouff, J. M., & Schutte, N. S. (2018). Meta-analysis of the efficacy of virtual reality exposure therapy for social anxiety. *Behaviour Change*, *35*(3), 152–166.

Choi, C. W., Honeycutt, J. M., & Bodie, G. D. (2015). Effects of imagined interactions and rehearsal on speaking performance. *Communication Education*, *64*(1), 25–44.

Cohen, L., & Huppert, J. D. (2018). Positive Emotions and Social Anxiety: The Unique Role of Pride. *Cognitive Therapy and Research*, *42*(4), 524–538. https://doi.org/10.1007/s10608-018-9900-2.

De Grez, L. (2009). *Optimizing the instructional environment to learn presentation skills* (Doctoral dissertation). Ghent University, Faculty of Psychology and Educational Sciences, Ghent, Belgium.

Denizci Nazligul, M., Yilmaz, M., Gulec, U., Yilmaz, A. E., Isler, V., O'Connor, R. V., Gozcu, M. A., & Clarke, P. (2019). Interactive three-dimensional virtual environment to reduce the public speaking anxiety levels of novice software engineers. *IET Software*, *13*(2), 152–158. https://doi.org/10.1049/iet-sen.2018.5140.

England, E. L., Herbert, J. D., Forman, E. M., Rabin, S. J., Juarascio, A., & Goldstein, S. P. (2012). Acceptance-based exposure therapy for public speaking anxiety.

Journal of Contextual Behavioral Science, *1*(1), 66–72. https://doi.org/https://doi.org/10.1016/j.jcbs.2012.07.001.

Fabris, C. P., Rathner, J. A., Fong, A. Y., & Sevigny, C. P. (2019). Virtual reality in higher education. *International Journal of Innovation in Science and Mathematics Education*, *27*(8), 69–80.

Fetscherin, M., & Lattemann, C. (2008). User acceptance of virtual worlds. *Journal of electronic commerce research*, *9*(3), 231.

Fodor, L. A., Coteț, C. D., Cuijpers, P., Szamoskozi, Ș., David, D., & Cristea, I. A. (2018). The effectiveness of virtual reality based interventions for symptoms of anxiety and depression: A meta-analysis. *Scientific Reports*, *8*(1), 10323.

Fredrickson, B. L. (2001). The role of positive emotions in positive psychology. The broaden-and-build theory of positive emotions. *The American Psychologist*, *56*(3), 218–226. https://doi.org/10.1037//0003-066x.56.3.218.

Gibson, L. A., & Sodeman, W. A. (2014). Millennials and technology: Addressing the communication gap in education and practice. *Organization Development Journal*, *32*(4), 63–75.

Gray, F. E. (2010). Specific oral communication skills desired in new accountancy graduates. *Business Communication Quarterly*, *73*(1), 40–67.

Greenwald, S., Kulik, A., Kunert, A., Beck, S., Fröhlich, B., Cobb, S. V. G., Parsons, S., Newbutt, N., Gouveia, C., Cook, C., Snyder, A., Payne, S., Holland, J., Buessing, S., Fields, G., Corning, W., Lee, V., Xia, L., & Maes, P. (2017). Technology and applications for collaborative learning in virtual reality. In *Proceedings of the 12th International Conference on Computer Supported Collaborative Learning (CSCL)*. Philadelphia, PA.

Grieve, R., Woodley, J., Hunt, S. E., & McKay, A. (2021). Student fears of oral presentations and public speaking in higher education: a qualitative survey. *Journal of Further and Higher Education*, *45*(9), 1281–1293. https://doi.org/10.1080/0309877x.2021.1948509.

Harris, S. R., Kemmerling, R. L., & North, M. M. (2002). Brief virtual reality therapy for public speaking anxiety. *Cyberpsychology & Behavior*, *5*(6), 543–550.

Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of educational research*, *77*(1), 81–112.

Heimberg, R. G. (2002). Cognitive-behavioral therapy for social anxiety disorder: current status and future directions. *Biological Psychiatry*, *51*(1), 101–108. https://www.biologicalpsychiatryjournal.com/article/S0006-3223(01)01183-0/fulltext.

Heimberg, R. G., Salzman, D. G., Holt, C. S., & Blendell, K. A. (1993). Cognitive-behavioral group treatment for social phobia: Effectiveness at five-year followup. *Cognitive Therapy and Research*, *17*(4), 325–339. https://doi.org/10.1007/BF01177658.

Hernandez-de-Menendez, M., Escobar Díaz, C. A., & Morales-Menendez, R. (2020). Educational experiences with Generation Z. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *14*(3), 847–859. https://doi.org/10.1007/s12008-020-00674-9.

Hinojo-Lucena, F. J., Aznar-Diaz, I., Caceres-Reche, M. P., Trujillo-Torres, J. M., & Romero-Rodriguez, J. M. (2020). Virtual Reality Treatment for Public Speaking Anxiety in Students. Advancements and Results in Personalized Medicine. *Journal of Personalized Medicine*, *10*(1). https://doi.org/10.3390/jpm10010014.

Hofmann, S. G., & DiBartolo, P. M. (2000). An instrument to assess self-statements during public speaking: Scale development and preliminary psychometric properties. *Behavior Therapy*, *31*(3), 499–515.

Jackson, D. (2010). An international profile of industry-relevant competencies and skill gaps in modern graduates. *International Journal of Management Education*, *8*(3), 29–58.

Lim, M. H., Aryadoust, V., & Esposito, G. (2023). A meta-analysis of the effect of virtual reality on reducing public speaking anxiety. *Current Psychology*, *42*(15), 12912–12928.

Lomas, C. W. (1937). The psychology of stage fright. *Quarterly Journal of Speech*, *23*(1), 35–44. https://doi.org/10.1080/00335633709391652.

McGovern, E., Moreira, G., & Luna-Nevarez, C. (2019). An application of virtual reality in education: Can this technology enhance the quality of students' learning experience? *Journal of Education for Business*, *95*(7), 490–496. https://doi.org/10.1080/08832323.2019.1703096.

Menzel, K. E., & Carrell, L. J. (1994). The relationship between preparation and performance in public speaking. *Communication Education*, *43*(1), 17–26.

Merchant, Z., Goetz, E. T., Cifuentes, L., Keeney-Kennicutt, W., & Davis, T. J. (2014). Effectiveness of virtual reality-based instruction on students' learning outcomes in K-12 and higher education: A meta-analysis. *Computers & Education*, *70*, 29–40.

Moskal, P., Ellis, T., & Keon, T. (2008). Summary of assessment in higher education and the management of student-learning data. *Academy of Management Learning & Education*, *7*(2), 269–278.

Palmas, F., Cichor, J., Plecher, D. A., & Klinker, G. (2019). Acceptance and effectiveness of a virtual reality public speaking training. In *Proceedings - 2019 IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2019* (pp. 363–371). Article 8943733 (Proceedings - 2019 IEEE International Symposium on Mixed and Augmented Reality, ISMAR 2019). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/ISMAR.2019.00034.

Palmas, F., Niermann, P. F. J., Plecher, D. A., & Klinker, G. (2022). Extended Reality Training for Business and Education: The New Generation of Learning Experiences. In *Proceedings - 2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct, ISMAR-Adjunct 2022* (pp. 322–326). (Proceedings - 2022 IEEE International Symposium on Mixed and Augmented Reality Adjunct, ISMAR-Adjunct 2022). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/ISMAR-Adjunct57072.2022.00071.

Palmas, F., Reinelt, R., Cichor, J. E., Plecher, D. A., & Klinker, G. (2021). Virtual Reality Public Speaking Training: Experimental Evaluation of Direct Feedback Technology Acceptance. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)* (pp. 463–472). https://doi.org/10.1109/VR50410.2021.00070.

Petronzi, R., & Petronzi, D. (2020). The Online and Campus (OaC) Model as a Sustainable Blended Approach to Teaching and Learning in Higher Education: A Response to COVID-19. *Journal of Pedagogical Research*, *4*(4), 498–507.

Poeschl, S. (2017). Virtual Reality Training for Public Speaking—A QUEST-VR Framework Validation. *Frontiers in ICT*, *4*. https://doi.org/10.3389/fict.2017.00013.

Ponniah, K., & Hollon, S. D. (2008). Empirically supported psychological interventions for social phobia in adults: a qualitative review of randomized controlled trials. *Psychological Medicine*, *38*(1), 3–14. https://doi.org/10.1017/S0033291707000918.

Powers, M. B., Sigmarsson, S. R., & Emmelkamp, P. M. G. (2008). A Meta–Analytic Review of Psychological Treatments for Social Anxiety Disorder. *International Journal of Cognitive Therapy*, *1*(2), 94–113. https://doi.org/10.1680/ijct.2008.1.2.94.

Premkumar, P., Heym, N., Anderson, P. L., Brown, D., & Sumich, A. (2022). The use of virtual-reality interventions in reducing anxiety. *Frontiers in Virtual Reality*, 3, Article 853678. https://doi.org/10.3389/frvir.2022.853678.

Premkumar, P., Heym, N., Brown, D. J., Battersby, S., Sumich, A., Huntington, B., Daly, R., & Zysk, E. (2021). The Effectiveness of Self-Guided Virtual-Reality Exposure Therapy for Public-Speaking Anxiety. *Frontiers in Psychiatry*, *12*, 694610. https://doi.org/10.3389/fpsyt.2021.694610.

Radianti, J., Majchrzak, T. A., Fromm, J., & Wohlgenannt, I. (2020). A systematic review of immersive virtual reality applications for higher education: Design elements, lessons learned, and research agenda. *Computers & Education*, *147*, 103778.

Reeves, R., Curran, D., Gleeson, A., & Hanna, D. (2022). A meta-analysis of the efficacy of virtual reality and in vivo exposure therapy as psychological interventions for public speaking anxiety. *Behavior Modification*, *46*(4), 937–965.

Rodebaugh, T. L., Holaway, R. M., & Heimberg, R. G. (2004). The treatment of social anxiety disorder. *Clinical Psychology Review*, *24*(7), 883–908.

Rodero, E., & Larrea, O. (2022). Virtual reality with distractors to overcome public speaking anxiety in university students. *Comunicar*, *30*(72), 87–99. https://doi.org/10.3916/c72-2022-07.

Šalkevičius, J., Miškinytė, A., & Navickas, L. (2019). Cloud Based Virtual Reality Exposure Therapy Service for Public Speaking Anxiety. *Information*, *10*(2). https://doi.org/10.3390/info10020062.

Sarpourian, F., Samad-Soltani, T., Moulaei, K., & Bahaadinbeigy, K. (2022). The effect of virtual reality therapy and counseling on students' public speaking anxiety. *Health Science Reports*, *5*(5), e816. https://doi.org/10.1002/hsr2.816.

Saxena, M., & Mishra, D. K. (2021). Gamification and Gen Z in higher education: A systematic review of literature. *International Journal of Information and Communication Technology Education (IJICTE)*, *17*(4), 1–22.

Schmid Mast, M., Kleinlogel, E. P., Tur, B., & Bachmann, M. (2018). The future of interpersonal skills development: Immersive virtual reality training with virtual humans. *Human Resource Development Quarterly*, *29*(2), 125–141. https://doi.org/10.1002/hrdq.21307.

Shute, V. J. (2008). Focus on formative feedback. *Review of educational research*, *78*(1), 153–189.

Slater, M., Gonzalez-Liencres, C., Haggard, P., Vinkers, C., Gregory-Clarke, R., Jelley, S., Watson, Z., Breen, G., Schwarz, R., & Steptoe, W. (2020). The ethics of realism in virtual and augmented reality. *Frontiers in Virtual Reality*, *1*, 1.

Smith, C. M., & Sodano, T. M. (2011). Integrating lecture capture as a teaching strategy to improve student presentation skills through self-assessment. *Active Learning in Higher Education*, *12*(3), 151–162.

Smith, T. E., & Frymier, A. B. (2006). Get 'real': Does practicing speeches before an audience improve performance? *Communication Quarterly*, *54*(1), 111–125.

Takac, M., Collett, J., Blom, K. J., Conduit, R., Rehm, I., & De Foe, A. (2019). Public speaking anxiety decreases within repeated virtual reality training sessions. *PLoS One*, *14*(5), e0216288. https://doi.org/10.1371/journal.pone.0216288.

Tse, A. Y. H. (2012). Glossophobia of university students in Malaysia. *International Journal of Asian Social Science*, *2*(11), 2061–2073.

Valls-Ratés, Ï., Niebuhr, O., & Prieto, P. (2022). Unguided virtual-reality training can enhance the oral presentation skills of high-school students. *Frontiers in Communication*, *7*. https://doi.org/10.3389/fcomm.2022.910952.

Valmaggia, L. R., Latif, L., Kempton, M. J., & Rus-Calafell, M. (2016). Virtual reality in the psychological treatment for mental health problems: An systematic

review of recent evidence. *Psychiatry Research*, *236*, 189–195. https://doi.org/10.1016/j.psychres.2016.01.015.

Van Ginkel, S., Gulikers, J., Biemans, H., & Mulder, M. (2015). Towards a set of design principles for developing oral presentation competence: A synthesis of research in higher education. *Educational Research Review*, *14*, 62–80.

Van Ginkel, S., Gulikers, J., Biemans, H., Noroozi, O., Roozen, M., Bos, T., van Tilborg, R., van Halteren, M., & Mulder, M. (2019). Fostering oral presentation competence through a virtual reality-based task for delivering feedback. *Computers & Education*, *134*, 78–97. https://doi.org/10.1016/j.compedu.2019.02.006.

Van Ginkel, S., Ruiz, D., Mononen, A., Karaman, C., Keijzer, A., & Sitthiworachart, J. (2020). The impact of computer-mediated immediate feedback on developing oral presentation skills: An exploratory study in virtual reality. *Journal of Computer Assisted Learning*, *36*(3), 412–422. https://doi.org/10.1111/jcal.12424.

Wallach, H. S., Safir, M. P., & Bar-Zvi, M. (2009). Virtual reality cognitive behavior therapy for public speaking anxiety: a randomized clinical trial. *Behavior Modification*, *33*(3), 314–338.

Wörtwein, T., Morency, L.-P., & Scherer, S. (2015). Automatic assessment and analysis of public speaking anxiety: A virtual audience case study. In *2015 International Conference on Affective Computing and Intelligent Interaction (ACII)* (pp. 187–193). IEEE. https://doi.org/10.1109/ACII.2015.7344570.

Yuen, E. K., Goetter, E. M., Stasio, M. J., Ash, P., Mansour, B., McNally, E., Sanchez, M., Hobar, E., Forte, S., Zulaica, K., & Watkins, J. (2019). A pilot of acceptance and commitment therapy for public speaking anxiety delivered with group videoconferencing and virtual reality exposure. *Journal of Contextual Behavioral Science*, *12*, 47–54. https://doi.org/10.1016/j.jcbs.2019.01.006.

Marek Górka*

Organizational Culture in the Context of Cybersecurity – Definitional Considerations

Abstract: Organizational culture plays a key role in the process of adapting to digital technologies. It promotes knowledge exchange among employees, which positively influences creativity and company performance. Digitalization, as a process conducive to knowledge sharing, enables the creation of more open and global informational spaces, which impacts institutional development. However, the increasing digitalization of society makes institutions vulnerable to cyber-attacks, highlighting the importance of established cybersecurity standards. Effective cybersecurity requires the integration of technology with appropriate user behaviors. Preventive measures and education in cybersecurity are crucial, especially in the context of growing digital threats. An organizational culture that promotes flexibility, collaboration, and employee education plays a significant role in adapting to digital technologies and managing risk. Digital transformation requires readiness for change, innovation, and collaboration. Technology companies demonstrate that an appropriate organizational culture fosters risk-taking and strengthens information security. Effective cybersecurity necessitates the integration of technical and behavioral aspects and understanding individual differences among employees. Contemporary challenges require a comprehensive approach, combining technology with appropriate user behaviors, to create a robust organizational culture that supports information security.

Keywords: organizational culture, cyber risk management, digital threats, cybersecurity, cyber resilience, behaviorism

Introduction

Technology is present in almost every aspect of human life, but understanding the changes it brings about is a significant contemporary challenge. Many research analyses observe the phenomenon of blurring boundaries between the virtual and physical worlds, which directly results in digital conditions affecting the real world (Stilman, 2020). Literature indicates that this situation is influenced, among other factors, by the existing divides between individuals raised in the digital era from birth and those who experienced childhood without today's technological scope (Prensky, 2012).

* *Faculty of Humanities, Koszalin University of Technology, ORCID: 0000-0002-6964-1581*

Within this process, there is a need to understand and analyze various aspects of functioning in an environment based on cyber technology. The digitally created reality, in which most of society currently participates, necessitates reflection on the changes occurring in society. Researchers point to the need to reassess the concept of social relationships in light of new technologies and changes in the way reality is constructed by cyber technology (Fisher, 2017; van der Kolk, 2014; Cabanas and Illouz, 2019). Many questions also arise about what might be destructive in modern progress and what are its negative aspects. Much of these concerns stem from attempts to understand the relationship between contemporary society and technology, provoking reflections on the concept of cybersecurity culture (Harari, 2017).

The processes of digitization and remote work, which have gained significance in recent years, further increase the risks associated with cybersecurity. Building and developing a cybersecurity culture is not only a necessity but also a crucial element of business strategy. This aims to protect against attacks, build customer trust, and meet regulatory requirements. Organizational culture in terms of cybersecurity must evolve to meet new challenges and threats. Such a culture not only protects the organization from potential attacks but also promotes innovative approaches to technology and crisis management. The goal of this article is to understand how cyber threats can stimulate innovation in organizations and how these experiences contribute to building a cybersecurity culture. The study focuses on analyzing crisis situations, identifying weaknesses in information systems, and on preventive and educational actions in the field of cybersecurity. To achieve these goals, the research reflection will be based on the analysis of the relevant literature and case studies. The literature review will cover scientific works and research reports on the impact of technology on social and individual life (Fisher, 2017; van der Kolk, 2014; Cabanas & Illouz, 2019). This analysis will allow for identifying key areas where technology exerts the greatest influence and understanding what changes occur in social relationships and ways of constructing reality through digital technologies.

Technology – Human

The relationships between humans and technology lead to various social implications that shape everyday life. Marshall McLuhan observed that technology is not separate from humans but is a continuation of their actions and thoughts, which has significant consequences for social and psychological interactions (McLuhan, 1994). Technology has become a medium and a message shaping society, human creativity, and enabling many people to express themselves. Therefore, studying

the impact of technology on culture and society is becoming increasingly important in the era of ever-evolving cyber culture.

For some users, the digital environment is completely natural and everyday, while for others it may be foreign or unsettling, even if they are familiar with and accept technology (Stilman, 2022). Questions are often raised about the consequences for society when it is socialized in an environment where active human interaction is lacking and replaced by technology (Thüring and Mahlke, 2007). These changes lead to a broader discussion about the relationship between humans and technology and to a greater understanding of the effects of its widespread use.

Digital progress, though concerning in some areas (such as crime or armed conflicts), is a significant step in human evolution, enabling control over one's biological and technological evolution. The change in the relationship between humans and technology has accelerated immensely in recent years, partly due to the introduction of new solutions such as touchscreens, voice and facial recognition technologies, and the use of biometric data (Wells and Usman, 2024). These technologies are characterized by ubiquitous data processing and connectivity, transforming the physical world into a digital one. Everyday life is rich with examples of such applications, e.g., personalized ads delivered to smartphones based on a customer's location or supermarket apps that continuously update inventory levels. With these changes, communication becomes increasingly personalized, simultaneously raising issues related to personal data protection. People are increasingly working virtually, using mobile devices connected to the network around the clock. These devices have become an integral part of life. However, the associated risks are becoming more real. Mobile apps constantly track people, raising concerns about privacy and data security, which also forces questions about the boundaries of privacy and surveillance. The COVID-19 pandemic has also accelerated this evolution, forcing many areas of life to move online.

Understanding and awareness of the threats posed by new technologies are key elements in building a secure cyberspace. At the same time, one must not forget about social aspects, such as protecting privacy and individual freedom in the digital era. Therefore, introducing innovations should be done in line with democratic and ethical values, which can contribute to building societal trust in both technology and the state.

However, the debate on this topic remains practical and does not address deeper issues related to human activity spheres such as security, privacy, risk, trust, usability, and flexibility. Thus, there is a need to characterize the cultural and social factors that shape the functionality of cyber technologies (Hilowle et al., 2019). Analysis in this area fills existing gaps in literature and provides a significant contribution to understanding the social determinants in the process

of human adaptation to cyber technologies. Research on complex issues related to cybersecurity, especially concerning the dimension of human adoption of new technologies in private or professional environments, is becoming increasingly significant for the surrounding reality.

Cybersecurity in the Social Dimension

Although technology brings numerous benefits, it also comes with challenges related to digital threats, which are becoming increasingly severe for all its users. In the context of many discussions and disputes provoked by today's digital reality, two dominant attitudes can be observed. The first is characterized by immense optimism regarding the potential benefits of technological progress. However, at the other end of the spectrum lies a cautious attitude, including skepticism and a critical approach to various ideas and concepts, including utopian visions of the future. These two opposing views are nothing new but shape discussions about the place and significance of cyber technologies in contemporary life.

Initially perceived as the domain of military strategists and IT specialists, cybersecurity has now become an area accessible to a broader community. This knowledge extends to decision-makers, diplomats, tech companies, activists, and scientists from various fields (Whyte, 2022). Cybersecurity has also become a recognized area of research in international relations and security studies, leading to an increase in the number of research centers and educational programs worldwide (Aradau, 2017; De Goede, 2018; Dunn Cavelty, 2018).

Currently, cybersecurity is an area of multidimensional development. However, to fully understand cybersecurity, it is valuable to consider it from both technical and social perspectives. On the one hand, there are technical possibilities such as network security and antivirus software. On the other hand, there is behavioral control concerning people and their actions. Nevertheless, there is a close relationship between them that cannot be separated (Stewart, 2020). Thus, there is a need for analysis of both technology and relevant behaviors. Without technology, flexible adaptation to growing needs and burdens cannot be ensured. However, without proper user behavior, even the most advanced technology may be ineffective. Therefore, it is crucial to integrate both elements to ensure comprehensive and effective cybersecurity. Focusing solely on one of these aspects does not allow for a full understanding of the current reality and its complex relationships. Recognizing these two spheres as fully legitimate elements is crucial, particularly in the process of detecting and preventing cyber threats (AlHogail, 2015; Dhillon et al., 2016).

Another equally important aspect of integration in the field of cybersecurity is the need to ensure digital resilience while maintaining the openness of the digital

environment, which is currently one of the greatest challenges facing political decision-makers. The effects of technological processes experienced in any region or organization can potentially cause problems in the entire interconnected global digital system. Therefore, the ongoing changes cannot be perceived solely on an individual or collective basis (Collett, 2021; Dunn Cavelty and Wenger, 2020, p. 8).

Responsibility for security has transcended the boundaries of individual IT teams, encompassing various institutions and numerous individuals, including over half of the world's population using the Internet. Additionally, the approach to security no longer focuses solely on technical aspects but increasingly considers legal and political aspects shaped by the diversity of cultures and customs (Baram et al., 2017; Cohen, 2017). Furthermore, studying the field of cybersecurity proves to be a significant challenge due to the dynamic processes occurring within it.

Organizational Culture

Organizational factors, such as flexible organizational culture, play a crucial role in the process of adapting to digital technologies. It fosters knowledge exchange among employees, which in turn positively impacts creativity and company performance. In the modern knowledge-based economy, the creation, sharing, and utilization of knowledge significantly influence enterprise productivity. Digitalization is a key element of this process. The competitiveness of companies is closely linked to their ability to utilize the latest technologies in business operations through effective knowledge utilization, leading to increased productivity (Martinez-Caro et al., 2020). Digitalization is a process inherently conducive to knowledge sharing, creating favorable conditions for information exchange beyond existing institutional and geographic boundaries, thereby forming a more open and global space where information can freely circulate, ultimately impacting institutional development (Ghosh et al., 2022). Currently, it is challenging to separate digitalization from organizational development strategies, as more entities are incorporating new technologies into their operations. Leveraging these solutions enables companies to embrace new business opportunities and enhance productivity (Eller et al., 2020).

With this premise in mind, it can be observed that digitalization allows for the expansion of existing knowledge within specific social groups and facilitates the streamlining of data processing and exchange, fostering the selection, integration, and transformation of previous assumptions. Furthermore, it encourages the pursuit of knowledge beyond boundaries, altering how these groups communicate and collaborate with external entities. This is particularly relevant in the context of cybersecurity, where rapid responses and flexibility are crucial for ensuring information security.

Contemporary organizations, as well as the digital infrastructure responsible for their operations, do not exist in isolation. The increasing digitization of society makes institutions increasingly vulnerable to cyberattacks. Already, most economic and administrative activities take place in digital environments, making attacks on these systems potentially devastating for entire organizations.

Understanding threats based on established cybersecurity standards within the organization is also important because the threat phenomenon is inherently continuous, requiring monitoring and adaptation to changing environmental conditions (Parida et al., 2016). Risk management encompasses a wide range of activities, including policy, procedure, and standard creation, as well as the enforcement of existing principles.

In the face of growing threats from cybercriminals, it is worthwhile to emphasize the role of preventive measures and continuous improvement in cybersecurity to effectively respond to evolving threats in the digital world. From an organizational perspective, it is crucial to adopt appropriate defensive practices that can effectively secure IT systems (Cenamor et al., 2019). An essential condition for efficient operation is also the creation of a shared vision and ambition regarding security throughout the organization, which can be achieved through employee engagement in goal and vision definition processes. Consequently, such actions promote anchoring changes and gradually building appropriate cybersecurity standards.

Organizational culture evolves based on collaboration and employees' experiences, constituting an integral part of the organization. Thus, although cybersecurity principles may be excellent and all employees may focus on them, a lack of teamwork and harmony within the team can lead to their ineffective implementation. Continuous adjustment of procedures to changing conditions and needs is therefore necessary, both among large enterprises and smaller entities (Ahmed et al., 2022). A similar situation may arise due to a lack of awareness and responsible behavior on the part of employees, which can undermine all efforts to ensure cybersecurity. Therefore, organizations should invest in education and training for their employees at all hierarchical levels to increase their awareness and skills in cybersecurity. Introducing training on the risks associated with immediate access to communication can be a key element in building actions conducive to strengthening cybersecurity. Furthermore, it is necessary to promote responsible use of technology and pay attention to data security priorities.

Assuming that each employee may have different levels of knowledge and skills, it is important to tailor training to specific needs and behaviors of employees. Not all individuals react in the same way to threats. Understanding these individual differences among employees and adapting educational offerings to

these differences can significantly increase the effectiveness of training programs. Inadequate employee education can lead to serious security gaps, resulting in the possibility of threats to the entire organization. Therefore, ensuring the comprehensiveness of training programs for staff is extremely important and can impact effective cybersecurity risk management.

Currently, as the issue of data security becomes increasingly pressing, it is important to understand human behavior and its impact on cybersecurity culture in organizations. Literature on the subject has analyzed the influence of the human factor on the use of cyber technology (Parsons et al., 2010). Research has noted that individual differences, personality traits, and cognitive abilities can significantly influence individuals' behavior, which in turn has consequences for organizational security. Human behavior may be susceptible to errors and impulsivity, leading to information security breaches. Partly, this situation may stem from the current reality where instant access to communication dominates through applications such as Skype, Microsoft Teams, Facebook Messenger, or WhatsApp. Understanding the impact of this phenomenon on cybersecurity culture in organizations is important. The ability to quickly access information and communicate via digital platforms contributes on the users' side to increased expectations for rapid responses. This immediate expectation for a response can lead to impulsive clicking and mismanagement of priorities, which can increase the risk of security breaches. Additionally, increasingly advanced applications use mechanisms such as the number of unread messages to prompt users to check their inboxes more frequently. This makes users of these applications more susceptible to phishing attacks and other forms of cyber threats.

So, a crucial aspect of organizational culture is understanding that people don't always adhere to security principles, even if they are aware of the threats. However, promoting responsible technology use and emphasizing the consequences of violating security principles are key issues. Assuming that the weakest link in the entire cybersecurity system is the human, the need for control and management of private devices in the workplace becomes particularly important. Even seemingly minor oversights can lead to serious consequences such as paralysis of the entire institution's functioning. Awareness of such situations among employees is crucial in building a cybersecurity culture because it helps understand why behavior needs to change and what benefits result from these changes (Kane et al., 2016; Lorenzo et al., 2022).

The risk of attacks exists regardless of the scale of operations, which is why increasing emphasis is placed on awareness-raising activities and building resilience to threats. Both large enterprises and startups require support in risk management and resilience building against cyber threats. However, a lack of adequate

budgets and limited access to cybersecurity experts can be challenging, especially for smaller entities.

One aspect of organizational culture is building trust and exchanging ideas and experiences among employees. Openness to communication and willingness to share suggestions are crucial for strengthening cybersecurity standards within an institution. Organizational values such as authenticity and integrity form the foundation of cybersecurity culture and should be reflected in the daily actions of employees. Contemporary organizational culture requires consideration of diverse perspectives and needs in the risk management process. Sharing ideas allows for increased awareness and understanding of various aspects of cyber threats. However, a significant challenge may be convincing employees that reporting any suspicious activities or situations is justified and appropriate, even if they may result from unconscious behaviors. The key to this is building trust and eliminating staff concerns about reprisals, which can be beneficial for the functioning of the entire institution (Eller et al., 2020; Martín-Peña et al., 2019).

In other words, organizational culture is not just a set of values but also the way they are implemented in daily organizational practice. The basis of this process is the clear definition of shared values and the conviction of their importance for achieving success. Cybersecurity procedures in an organization should be integrated with its daily practices and values, which are authentically adhered to by employees every day. An essential element of building this culture is openness to communication and willingness to share suggestions for improving actions related to cybersecurity.

Discussions on values in organizational culture can lead to reflections on how a company defines its goals and priorities. An example could be a situation where a manager declares that results are a priority but neglects aspects related to organizational culture. Such an approach can lead to the ignoring of significant factors that influence outcomes, such as employee engagement or safety concerns. Therefore, it is important for a company not only to focus solely on achieving results, such as the number of secured systems, but also on building an organizational culture that promotes awareness and engagement in cybersecurity. Values and norms influence interactions among employees, which fosters the creation of new management models in the cybersecurity field. Key elements of digital culture include continuous innovation in security, responsiveness to threats, openness to collaboration and knowledge sharing, and autonomy in decision-making regarding security.

Digital transformation is associated with the shaping of a new organizational identity. Therefore, entities should be open to change. Although not every reaction or stimulus leads to transformation, readiness for change is a cultural trait that

fosters continuous exploration of new solutions. Technological companies like Google, Meta, or Apple have shown that organizational culture promotes risk-taking, innovation, and collaboration in information security contexts (Grover, 2022; Rikap, 2023).

It is not enough to simply invest in advanced technologies; it is necessary to create an appropriate organizational culture that promotes awareness and responsibility in information security. An example could be the story of Colonel Paul Nakasone, who as the commander of a military cyber operations unit was asked to join a team tasked with dealing with increasingly complex cyber threats. In his statement, values such as trust, teamwork, cooperation, imagination, and creativity were emphasized, which played a crucial role in operational success (Nakasone, 2023). In practice, this means developing an organizational culture where every employee feels valued, supported, and safe.

It is important for organization leaders to understand that organizational culture plays a significant role in motivating employees to take actions for cybersecurity. Implementing initiatives such as cyber hygiene campaigns or promoting operational cooperation with the private sector can contribute to increased awareness and effectiveness of actions. As can be seen, organizational culture plays a crucial role in building resilience to cyber threats. It is a culture that recognizes that collaboration and mutual support are necessary for effectively combating these threats.

The culture of cybersecurity requires an understanding not only of the technology itself but also of the context in which decisions regarding data security are made. Awareness that even seemingly innocent actions in the workplace, such as social media postings or online gaming, can pose threats to data security and network infrastructure. Employers should therefore take actions aimed at educating employees about safe internet usage in the workplace and establishing clear rules regarding the use of company devices for personal purposes. Users often do not realize the risks associated with using illegal files or unsecured internet connections.

The development of technology and changes in work practices require new approaches to managing digital tools assigned to employees. The challenge here is to reconcile minimal security standards with flexibility in performing daily tasks. Another important challenge is to develop practices that are consistent in terms of control for all users, both remote and on-site workers.

It can be argued that as technology evolves and social needs change, the ongoing challenge will be both maintaining security and user comfort. To reconcile these expectations, cooperation and engagement of both employees and security specialists will be required. Such a dialogue in creating and implementing

appropriate procedures is one of the elements of building conditions conducive to stable development, including cybersecurity, in institutions. The lack of a defined culture can lead to the emergence of undesirable actions that may harm the organization.

It is also important for companies to change their approach to cybersecurity issues, not only treating this concept as a requirement arising from regulatory requirements but also as an integral element of the business strategy. Introducing standards and promoting the security cycle as an integral whole can change the perception of this area and contribute to more effective security practices in organizations. An approach based on prediction, proactivity, resilience, and continuous action becomes a key element of cybersecurity strategy for public institutions. It is important for both organizations and individuals to perceive security as a process of continuous improvement, rather than a one-time obligation. Additionally, it is important for the organization to treat security as an integral element of the business strategy. Finally, in the context of a dynamic and evolving cyber environment, promoting flexibility and adaptability in security practices becomes essential. Companies should be prepared to quickly respond to changing conditions and threats, which requires continuous monitoring, assessment, and updating of information security strategies.

The primary obligation of any organization is to ensure data protection and implement the concept of cyber resilience, which not only includes preventing attacks but also preparing for effective response and rapid recovery after an incident. In the field of cybersecurity, there are no ultimate solutions because the only constant is continuous change. Accepting this dynamic forces a focus on continuous improvement and preparation for potential incidents. Therefore, it is essential for organizations to shape their culture early in their development to avoid taking random and ill-considered actions that may lead to undesirable consequences.

Summary

The relationship between humans and technology significantly impacts society, shaping daily life and social interactions. Marshall McLuhan suggests that technology extends human actions and thoughts, influencing social and psychological interactions. Technology has become a key medium affecting society, culture, and human creativity, emphasizing the need for research on its impact on culture and society in the era of cybersecurity.

For some users, technology is a natural part of everyday life, while for others, it may be unsettling, despite accepting its presence. Questions arise about the social consequences of living in a technological environment where active interpersonal

interaction is lacking. These changes have accelerated with the introduction of new technologies such as touch screens, voice and face recognition technologies, and biometric data. Through ubiquitous data processing and connectivity, these technologies transform the physical world into a digital one.

The COVID-19 pandemic accelerated digital evolution, forcing many aspects of life to move online, highlighting the need to understand technological threats and protect individual privacy and freedom. The introduction of technological innovations should align with democratic and ethical values to build societal trust in technology.

Cybersecurity has become an important area of research in international relations and security studies, engaging a wide range of stakeholders, from military strategists to political decision-makers and activists. Effective cybersecurity requires the integration of technology and human behavior, emphasizing the need for education and training for users.

Organizations must adjust their cybersecurity strategies, considering the flexibility and collaboration of employees. The increasing digitization makes institutions more vulnerable to attacks, requiring continuous improvement and adaptation to evolving threats. Employee education and awareness are crucial for building an effective cybersecurity system.

Understanding human behavior and its impact on the culture of cybersecurity is essential for information security. Contemporary communication applications may increase the risk of security breaches by encouraging users to react quickly. Promoting responsible use of technology and awareness of threats is crucial for effective cyber risk management.

References

Ahmed, A., Bhatti, S. H., Gölgeci, I., & Arslan, A. (2022). Digital platform capability and organizational agility of emerging market manufacturing SMEs: The mediating role of intellectual capital and the moderating role of environmental dynamism. Technological Forecasting and Social Change, 177, 121513. doi:10.1016/j.techfore.2022.121513.

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567–575.

Aradau, C. (2017). Assembling (non) knowledge: Security, law, and surveillance in a digital world. International Political Sociology, 11(4), 327–342. https://doi.org/10.1093/ips/olx019.

Cabanas, E., & Illouz, E. (2019). Manufacturing happy citizens: How the science and industry of happiness controls our lives. Polity Press.

Cenamor, J., Parida, V., & Wincent, J. (2019). How entrepreneurial SMEs compete through digital platforms: The roles of digital platform capability, network capability, and ambidexterity. Journal of Business Research, 100, 196–206. doi:10.1016/j.jbusres.2019.03.035.

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. Journal of Cyber Policy, 6(3), 298–317.

De Goede, M., Bosma, E., & Pallister-Wilkins, P. (Eds.). (2019). Secrecy and methods in security research: A guide to qualitative fieldwork. London: Routledge.

Dhillon, G., Oliveira, T., Susarapu, S., & Caldeira, M. (2016). Deciding between information security and usability: Developing value-based objectives. Computers in Human Behavior, 61, 656–666.

Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. Politics and Governance, 6(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Eller, R., Alford, P., Kallmünzer, A., & Peters, M. (2020). Antecedents, consequences, and challenges of small and medium-sized enterprise digitalization. Journal of Business Research, 112, 119–127. doi:10.1016/j.jbusres.2020.03.004.

Fisher, J. (2017). Healing the fragmented selves of trauma survivors: Overcoming internal self-alienation. Routledge.

Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. Technovation, 113, 102414. doi:10.1016/j.technovation.2021.102414.

Grover, V. (2022). Digital agility: Responding to digital opportunities. European Journal of Information Systems, 31(6).

Harari, Y. N. (2017). Homo Deus: A brief history of tomorrow. Penguin.

Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2023). Users' adoption of national digital identity systems: Human-centric cybersecurity review. Journal of Computer Information Systems, 63(5), 1264–1279. doi:10.1080/08874417.2022.2140089.

Kane, G. C., Palmer, D., Phillips, A. N., & Buckley, N. (2016). Aligning the organization for its digital future. MIT Sloan Management Review, 58(1), 1–30.

Lorenzo, D., Núñez-Cacho, P., Akhter, N., & Chirico, F. (2022). Why are some family firms not innovative? Innovation barriers and path dependence in family firms. Scandinavian Journal of Management, 38(1), 101182. doi:10.1016/j.scaman.2021.101182.

Martín-Peña, M. L., Sánchez-López, J. M., & Díaz-Garrido, E. (2019). Servitization and digitalization in manufacturing: The influence on firm performance. Journal of Business & Industrial Marketing, 35(3), 564–574. doi:10.1108/JBIM-12-2018-0400.

Mcluhan, M. (1994). Understanding media: The extensions of man. The MIT Press.

Nakasone, P. A front row view of the NSA: Reflections from General Paul M. Nakasone. Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/front-row-view-nsa-reflections-general-paul-m-nakasone.

Parida, V., Patel, P. C., Wincent, J., & Kohtamäki, M. (2016). Network partner diversity, network capability, and sales growth in small firms. Journal of Business Research, 69(6), 2113–2117. doi:10.1016/j.jbusres.2015.12.017.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: Individual, culture, and security environment. Defense Technical Information Center.

Prensky, M. R. (2012). From digital natives to digital wisdom: Introduction. https://marcprensky.com/writing/Prensky-Intro_to_From_DN_to_DW.pdf.

Reddy, R. C., Bhattacharjee, B., Mishra, D., & Mandal, A. (2022). A systematic literature review towards a conceptual framework for enablers and barriers of an enterprise data science strategy. Information Systems and e-Business Management, 20(1), 223–255. doi:10.1007/s10257-022-00550-x.

Rikap, C. (2023). The expansionary strategies of intellectual monopolies: Google and the digitalization of healthcare. Economy and Society, 52(1).

Stewart, H. (2020). Information technology and cyber security unplugged: The interrelationship between human technology and cyber crime today (English ed.). Virginia - USA: Rohhat LTD.

Stilman, R. (2020). i-Self: Accounting for our digital identity. The Transactional Analyst, 10(1), 8–10.

Stilman, R. (2022). Attached to technology: Exploring identity and human relating in a virtual and corporeal world. Transactional Analysis Journal, 52(2), 93–105. doi:10.1080/03621537.2022.2036484.

Thüring, M., & Mahlke, S. (2007). Usability, aesthetics and emotions in human–technology interaction. International Journal of Psychology, 42(4), 253–264.

van der Kolk, B. (2014). The body keeps the score: Brain, mind, and body in the healing of trauma. Penguin.

Wells, A., & Usman, A. B. (2024). Privacy and biometrics for smart healthcare systems: Attacks, and techniques. Information Security Journal: A Global Perspective, 33(3), 307–331.

Whyte, J. (2022). Cybersecurity, race, and the politics of truth. Security Dialogue, 53(4), 342–362. https://doi.org/10.1177/096701062211017.

Shobhit Agarwal, Bozena Lamek-Creutz*

Artificial Intelligence as an Automation Tool in Manufacturing Industry

Abstract: Over the last few decades, the integration of artificial intelligence (AI) into manufacturing industries has seen amazing improvements, revolutionizing traditional manufacturing procedures and redefining the landscape of industrial automation. This paper delves into the transformative role of artificial intelligence (AI) as an automation tool in the manufacturing industry, a sector pivotal to economic growth and innovation. By integrating AI, particularly through advancements in computer vision (CV) and tiny machine learning (TinyML), manufacturing processes are experiencing unprecedented improvements in efficiency, precision, and adaptability. The paper provides a comprehensive overview of AI-driven applications such as safety monitoring, predictive maintenance, and quality control. In particular, the study focuses on the challenges and opportunities presented by deploying AI in resource-constrained environments, showcasing the potential of TinyML to offer cost-effective solutions without compromising performance. The discussion is enriched by two detailed case studies: one involving FESTO's Cyber-Physical System for PCB quality control, and another highlighting the application of TinyML for quality control for metal welding process. These case studies illustrate the practical benefits of AI integration, including reduced inspection time, cost savings, scalability, and enhanced product quality. Moreover, the paper addresses the broader implications of AI in driving the Industry 4.0 revolution, where interconnected, adaptive, and intelligent systems are expected to dominate future manufacturing landscapes.

Keywords: *Quality Control, Artificial Intelligence, Manufacturing, Automation*

1. Introduction

1.1 History of Artificial Intelligence

The term artificial intelligence (AI) was officially coined in the summer of 1956, during the Dartmouth Conference by John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon [McCarthy et al., 2006]. The conference is sometimes referred to as the "birthplace of AI" because it organized and stimulated the field. Throughout the following decades, AI research went through various phases, including periods of optimism and significant breakthroughs known as "AI Summers". As well as phases of reduced funding and reduced interest, often

* *Duale Hochschule Baden-Württemberg Mannheim*

referred to as "AI winters" [Toosi et al., 2021]. Another key figure in the early inception of AI was the British mathematician Alan Turing. In the 1950s, he published a paper titled "Computers and intelligence", where he talked about a tool to distinguish between a task carried out by a machine and one carried out by a human. The test is famously known as the "Turing test", which consists of a set of questions that must be answered. However, the term AI was coined around six years after Turing's paper [Turing, 1950]. The test is still used today on the internet as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart).

A brief history of Machine learning & Deep learning: After the introduction of the "Turing test" in 1950 and the official inception of the field of AI in 1956. The first major event was Rosenblatt's Perceptron algorithm [Rosenblatt, 1958]. This was the first algorithm and implementation to train a single linear operation on a 'neuron'. This was followed by Arthur Samuel's work in 1959 on developing a computer program that could play checkers. Arthur Samuel is also credited with proposing the term "machine learning" (ML) [Samuel, 1959]. However, the limitations of single-layer perceptrons were later on highlighted by [Minsky and Papert, 1969]. This led to the first "AI winter". Thereafter, in the 1980s, there was a resurgence in machine learning research largely due to the development of multi-layer neural networks and the introduction of the backpropagation algorithm [Rumelhart et al., 1986]. The following period also saw the emergence of new machine learning algorithms such as support vector machines [Hearst et al., 1998] and decision trees [Quinlan, 1986] etc. During the 1990s, machine learning began to gain traction in practical applications, spurred by the increasing availability of data and computational power.

The 2000s saw a significant shift in machine learning research with the introduction of deep learning [LeCun et al., 2015]. A sub-field within machine learning that focuses on deep neural networks i.e., neural networks with multiple layers. The term "deep learning" was popularized by Geoffrey Hinton, although the underlying concepts date back to the earlier work on neural networks. A break-through with practical deep learning came from Alexnet [Krizhevsky et al., 2012]. This was among the first convolutional neural networks (CNN) that was trained on the graphics processing unit (GPU) and had won the ImageNet Challenge. This event marked the beginning of deep learning's dominance in various AI fields, including computer vision (CV), natural language processing, and speech recognition. From 2012 to the present day, deep learning has continued to advance rapidly, with the development of more sophisticated architectures like generative adversarial networks (GANs) [Goodfellow et al., 2014], gated recurrent units (GRU) [Chung et al., 2014], and transformers

and attention mechanisms [Vaswani et al., 2017]. These advancements have enabled a new stream of research around foundation models [Bommasani et al., 2022], one of the prominent examples of foundation models is the Generative pre-trained transformer (GPT) which was popularized by the chatbot called chatGPT [OpenAI, 2023].

1.2 Manufacturing & AI

The manufacturing industry is key to any industrialized economy, it not only contributes to gross domestic product (GDP) but also creates high-paying jobs and creates a trickle-down effect on economic benefits. It is also closely linked to innovation, science, technology, engineering, and mathematics [Wang, 2018]. In the context of this study, the manufacturing industries are the industries that are equipped with heavy machinery and digital tools. Apart from its role in being the cornerstone for economic growth. Manufacturing industries are also important for a nation's sustainable economic growth. However, the manufacturing industries are usually traditional and changes are slow and costly [Jaeger and Upadhyay, 2020]. They are also exceptionally complex, where multiple things have to happen in the correct order to produce high-quality products for the customers [Kovalenko et al., 2023]. The manufacturing industry is often slow to adopt new technologies for a variety of reasons. A few common barriers identified are resource availability, lack of knowledge, lack of skills, lack of technological, and strategic expertise and skilled workforce [Andreas Kornmaaler Hansen and Lassen, 2024]. Lastly, the authors in [Ghobakhloo et al., 2022] have pointed out that there is an even slower rate of technology adoption in SMEs and this has been pointed out by numerous studies. However, in the last decade, a greater degree of digitalization has been transforming industrial production systems resulting in 'The fourth industrial revolution' or 'Industry 4.0' [Carla Gon¸calves Machado and da Silva, 2020]. The central element of 'Industry 4.0' is smart manufacturing [Klingenberg, 2017]. Smart manufacturing takes a wider view of factories as being part of the whole life cycle of the product [Frank et al., 2019].

A brief history of Manufacturing & AI: Some of the earliest work on manufacturing and AI dates back to the mid-1980s. When AI was in its initial phase data storage and computation were expensive. One of the first papers on manufacturing and AI discussed how it can be used in process execution, shop floor diagnosis systems, process diagnosis systems, and knowledge-based simulations [Kempf, 1985]. Another study discussed how AI can be used for control functions in manufacturing, the authors also deployed a simple neural

network with 10 inputs, 51 hidden units, and 22 outputs [Rabelo and Alptekin, 1989]. In the late 1990s and early 2000s, there was a plethora of research in the field. For example, scheduling of products using AI [Rodríguez-Somoza et al., 1990], distributed AI in industry [Parunak, 1996], applications of neural networks [Zhang and Huang, 1995], application of AI in FMS (Flexible Assembly Systems) simulation and scheduling [Kovács, 1997] & AI tools for decision support [Chan et al., 2000] etc. Since late the 2010s, with the advent of deep learning and cheaper computation costs, AI applications in manufacturing have witnessed a steep rise.

1.3 AI based automation in manufacturing

There have been various studies on the application of AI in manufacturing [Plathottam et al., 2023], [Mypati et al., 2023], [Wan et al., 2020] & [Xu et al., 2022] etc. An overview of possible application areas for automation is 1. Production planning and demand forecasting, 2. Safety and monitoring, 3. Designing and manufacturing, 4. Defects detection, 5. Quality Control, 6. Predictive Maintenance, 7. Supply chain monitoring etc. [Javaid et al., 2022]. The following section will explore state-of-the-art (SOTA) AI methods and technologies for some of the aforementioned application areas.

1. Safety and monitoring: Intelligent Monitoring Systems (IMS) have become essential in today's fast-paced manufacturing industry. They provide real-time information on equipment performance, production processes, and quality assurance. These systems enable proactive decision-making and production process optimization by gathering and analyzing data from a variety of sensors and devices within the manufacturing environment. IMS employs a variety of AI and ML algorithms to analyze this real-time data [Ani et al., 2024]. Additionally, the authors in [Ding et al., 2020] talk about industrial artificial intelligence (IAI), which takes a wholesome overview of available AI technology for a variety of tasks including production monitoring. Furthermore, robustness and safety are essential for industrial production [Zheng et al., 2016]. To address the issue of safety in collaborative workspace between humans and robots. A safety system based on fuzzy logic and SOTA deep learning algorithm was presented by [Hata et al., 2019]. As Industry 4.0 has shifted towards autonomous or semi-autonomous systems, there is a need for safety checks. The authors in [McDermid et al., 2019] provide a comprehensive framework for AI/ML-based solutions. Lastly, a general-purpose solution for AI-based safety was proposed by [Gheraibia et al., 2019]. Where a decision tree-based solution is employed to correctly classify abnormal behaviour.

2. Predictive Maintenance: In the fastmoving manufacturing space, the capacity to predict the maintenance needs of the future is a major challenge. The ability to correctly predict future maintenance needs can have many positive effects such as lower costs, better control, lower machine downtime and, increased quality of the production [Zonta et al., 2020]. Predictive maintenance (PdM) is a historic data-driven maintenance strategy. It originates from the idea of preventive maintenance. The primary focus of PdM is to improve the performance and efficiency of manufacturing by increasing the life span of equipment [Achouch et al., 2022]. PdM aims to predict usage patterns and trends, usually machine or deep learning models are used to forecast the pending failures ultimately helping the decision-making process [Sezer et al., 2018]. In the recent past PdM has emerged as a common aim across industries to reduce maintenance costs and to support operational management in a sustainable manner [Ayvaz and Alpay, 2021].
3. Quality Control: The quality of a product is defined as the attainment of certain specifications or the requirements of the customer, without any defect [Judi et al., 2011]. There have been numerous studies on quality control (QC) in the field of manufacturing and there is unanimous agreement on the importance of QC [Escobar and Morales-Menendez, 2018] and [Ryabchik et al., 2019]. One of the most common QC implementations is visual inspection via computer vision (CV). CV has a wide range of applications, from image generation to performing quality control in manufacturing. For example, a study on how CV can be applied for quality control of 3D printed parts was presented by [Akundi and Reyna, 2021]. An autoencoder-based solution for defect detection in fabric manufacturing was presented by [Chen et al., 2021]. A deep-learning-based CV model for defect detection in the welding process was presented by [Xia et al., 2020]. Additionally, [Sharma and Kumar, 2024] showed how CV can be deployed to perform quality control in PCB board manufacturing. Given the importance of QC for the manufacturing industries. The primary focus of this study is CV-based QC. The layout of the remainder of this work is as follows: Section 2 provides a brief literature review and Section 3 provides two real-world case studies on CV-based quality control applications.

2. Literature & Related work

2.1 Computer vision

Humans seem to have little trouble understanding the three-dimensional structure of the environment around them. Consider how clear your perception of the three dimensions is when you gaze at anything. Humans can easily distinguish the

scene from the background thanks to the delicate patterns of light and shade that reveal the shape and depth of things [Szeliski, 2010]. However, this phenomenon of visual perception is difficult for computers to translate [Papert, 1966]. Hence, a new research field of CV got its inception. Computer vision as a technology has two objectives. From the perspective of biological research, CV seeks to develop computational models of the human visual system. From an engineering perspective, CV seeks to create autonomous systems that are capable of carrying out some of the tasks that the human visual system can do [Huang, 1996]. Early compute vision studies date back to the 1960s when the technology was first used by [Roberts, 1963]. The author talked about how 2D perspective views of blocks may be used to extract 3D geometrical information.

The early days of CV research involved a two-stage process where, firstly, information or features were extracted from the image, and then these features were used as input for further tasks. The major flaw in this approach are these 'handcrafted features', as the absolute or final accuracy of the downstream task was heavily dependent on the quality of the extracted features [Rawat and Wang, 2017]. However, the more traditional methods were replaced with convolutional networks, and one of the earliest works on CNNs was presented by [LeCun et al., 1998]. Furthermore, the introduction of ImageNet [Deng et al., 2009] and ImageNet Large Scale Visual Recognition Challenge (ILSVRC) sparked a revolution in CV research. The first winner of ILSVRC using CNNs was Alexnet [Krizhevsky et al., 2012]. Since the release of Alexnet, convolutional neural networks have become the de facto standard models for CV tasks. Alexnet was among the earliest models to be trained on a GPU, and in the following years various other models were proposed, such as ResNet [He et al., 2015], Inception [Szegedy et al., 2014], VGG [Simonyan and Zisserman, 2015], DenseNet [Huang et al., 2018] and many more. Additionally, the recent developments in the field of deep learning, and particularly the advancements in the field of DCNNs (Deep Convolutional Neural Networks) have made them the dominant architecture for object recognition, image classification, and image segmentation tasks.

2.2 Challenges to CV

Modern-day CV is often synonymous with CNNs, as they form the backbone of almost all of the recent CV solutions. However, CNN faces a multitude of challenges. One major hurdle with CV is data availability. The authors [Liu and Du, 2024] underline how the lack of data negatively impacts CV research in the field of biomedicine. However, this problem is not only limited to the biomedical field. In industrial settings as well, data availability and data quality are big challenges

[Bai et al., 2023]. Another challenge with CNNs is the problem of data imbalance or sparsity/lack of certain examples. The imbalance between data points and their effects on the overall results of computer vision tasks was discussed by [Sampath et al., 2021]. This problem is easily overlooked in datasets frequently used in research, as they tend to have balanced statistics regarding target class distribution. However, real-world data sets, especially for quality control in manufacturing, are very different, as collecting negative samples is difficult. Leading to an imbalance in the dataset. Furthermore, the main challenges for the application of CV to real-world industrial data can be enumerated as 1. Visual accessibility, 2. Labelling, 3. Gathering faulty data/Imbalance, 4. Lighting, 5. Noise, 6. Sensor Failure, 7. Pose/Posture, 8. Appearance change [Leyendecker et al., 2023].

2.3 TinyML

There has been a substantial amount of research focused on embedded technologies in the recent past. The main motivation is the resource-constrained environments in which real-world applications take place. Embedded technologies can provide real-time solutions for complex problems [Dutta and Bharali, 2021]. In the context of AI-based solutions as the size of models and parameters increases, the cost of training and inference also increases. To the opposite end of large models are models that are scaled down to a few thousand or maybe a few hundred parameters that are designed to run on microcontrollers. This paradigm of AI is known as TinyML (Tiny Machine Learning) [Warden and Situnayake, 2019]. Furthermore, there are two strategies to operationalize an AI model. Either to deploy on a cloud-based solution (expensive and versatile) or deploy on the edge (limited computation capacity and quicker inferences). A software engineering-oriented example of TinyML was presented by [Lakshman and Eisty, 2022]. The authors highlight the need for more research into new approaches that can scale CV applications on TinyML platforms. Another example of TinyML is where the authors use CNN-based models for anomaly detection in plastic components [Albanese et al., 2023]. There has been substantial research in the field of TinyML, with various authors highlighting its potential for future applications, such as [Kallimani et al., 2024] and [Abadade et al., 2023]. Both large models and TinyML have their advantages and disadvantages and have an important place in CV-based quality control.

3. Case Studies

The following section explores two case studies of CV-cased QC. Each study explores a different application scenario.

3.1 FESTO's Cyber-physical System

1. Introduction: In the rapidly evolving electronics industry, ensuring the quality of printed circuit boards (PCBs) is crucial. Defective PCBs can lead to significant failures in electronic devices, making quality control a top priority for manufacturers. Traditional methods of quality inspection are often manual and prone to human error. This case study explores how Festo's Cyber-Physical System [Festo, 2021a], equipped with a camera inspection module, can be used to perform the quality control process on PCBs.
2. Objective: The objective of this case study was to explore a CV-based quality control system for PCB boards using Festo's Cyber-Physical System (CPS). The system was designed to detect defects such as missing components, misalignments, and soldering issues on PCBs. The CPS utilized a camera inspection module integrated with CV algorithms to identify and classify defects, ensuring high precision and reliability.
3. System Components:
    1. Festo CP Factory: The backbone of the system, the CP Factory is a modular and flexible Industry 4.0 learning and research platform. It simulates a real production environment with integrated cyber-physical systems, allowing for the automation of manufacturing processes.
    2. Camera Inspection Module: A high-resolution camera system was integrated into the CPS to capture detailed images of the PCBs as they moved through the conveyor belt. This module was critical in the collection of data.
    3. Computer vision Algorithms: Advanced CV models were trained on a dataset of collected PCB images with labelled defects. These models were then operationalized to analyze the images captured by the camera and classify the defects.
    4. Communication Protocols: The system was equipped with robust communication protocols to enable seamless data exchange between the camera module, the processing unit, and the control systems.
4. Implementation Process:
    1. Dataset Preparation: A comprehensive dataset of PCB images was compiled using the camera module, containing examples of both defect-free and defective boards. Defects included missing components, misaligned parts, and soldering errors. Each image was labelled to facilitate the training of machine learning models.
    2. Model Training and Optimization: The images were used to train a group of convolutional neural networks (CNN) that could accurately detect and

classify defects. The model was optimized for performance, ensuring it could operate within the real-time constraints of the production line.

3. System Integration: The trained model was not directly integrated into the Festo CPS. The camera inspection module was installed on the production line, positioned to capture images of each PCB as it moved through the system. The camera module then would send the image data to the connected computer where the CV model was executed. This relay of information was facilitated via the Manufacturing Execution System (MES).
4. Testing and Evaluation: The system was tested in a controlled environment, with various PCB boards passing through the production line. The accuracy and speed of the defect detection process were evaluated, with the system achieving an accuracy rate of about 95% in identifying defects.

Fig. 1: Cyber-Physical Lab [Festo, 2021b]

(a) Camera module (b) CP Lab station

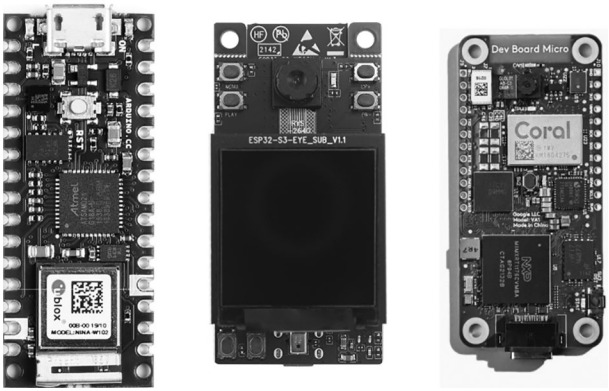
5. Key takeaways:
   1. Reduced Inspection Time: Automated inspection can reduce the time required to inspect each PCB, allowing the production line to operate at higher speeds without compromising quality.
   2. Cost Savings: By identifying defects early in the production process, the system can minimize the need for costly rework and scrap, leading to substantial cost savings.
   3. Scalability: The modular nature of the Festo CPS allowed for easy scaling of the system, enabling it to handle increased production volumes as needed.
   4. Conclusion and Future Work: The successful implementation of this case study with the camera inspection module demonstrated the potential of

CV-based technology in enhancing quality control processes in PCB manufacturing. The integration of CV algorithms with high-resolution camera systems enabled real-time, automated defect detection, significantly improving production efficiency and product quality. Future work could involve further optimization of the CV models to improve defect classification accuracy and reduce inspection times. Additionally, expanding the system to include predictive maintenance capabilities could further enhance the reliability and efficiency of the production line.

3.2 TinyML based quality control

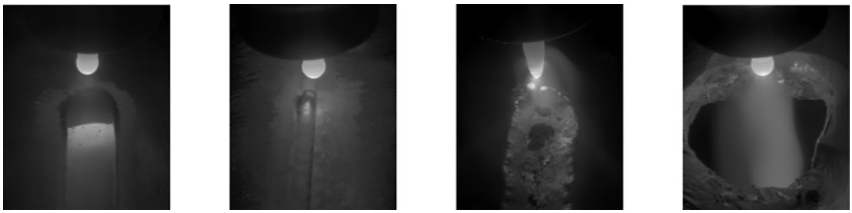
1. Background: Quality control in manufacturing traditionally relies on powerful hardware to run machine learning models for product inspection and machine monitoring. However, this approach can be prohibitively expensive, particularly for small or resource-constrained manufacturers. Tiny Machine Learning (TinyML) offers a solution by enabling the deployment of machine learning models on low-cost microcontrollers, which consume minimal power and have limited memory. This study demonstrates the feasibility of using TinyML for image-based quality control in manufacturing.
2. Project Overview: The project aimed to develop a TinyML solution for detecting production errors in a manufacturing setting. Specifically, the team focused on implementing an image classification model capable of identifying defects in products. This involved training, optimizing, and deploying the model on a microcontroller to ensure it could operate effectively within the hardware's constraints.
3. Hardware Selection: The hardware chosen for this project was the Arduino Nano 33, equipped with 256 kB RAM, 1 MB Flash, and a 64 MHz CPU. This microcontroller was selected due to its affordability and compatibility with the TinyML framework. While the Arduino Nano 33 served as the primary platform, the project also noted that more powerful alternatives like the ESP32 or the Coral Devboard could be used to improve performance.
4. Dataset and Model Development:
   – The dataset used for training the model was the TIG Aluminium 5083 dataset, which contains images of welding defects. To fit the microcontroller's limited resources, the images were resized to 64x64 pixels, reducing the number of features the model needed to process. The model was a custom convolutional neural network (CNN), specifically designed to be small enough to run on the Arduino Nano 33.

Fig. 2: There were three available microcontrollers, 1. Arduino Nano 33 [Arduino, 2019], 2. ESP32 EYE [Systems, 2023], 3. Coral Dev Board Micro [coral.ai, 2022]. In this case study an Arduino Nano 33 was utilized



(a) Arduino Nano (b) ESP32 EYE (c) Coral Devboard

Fig. 3: Exemplary images from TIG welding Al-5083 dataset [Bacioiu et al., 2019] where the (a) shows a correct weld and (b,c,d) various types of incorrect welds

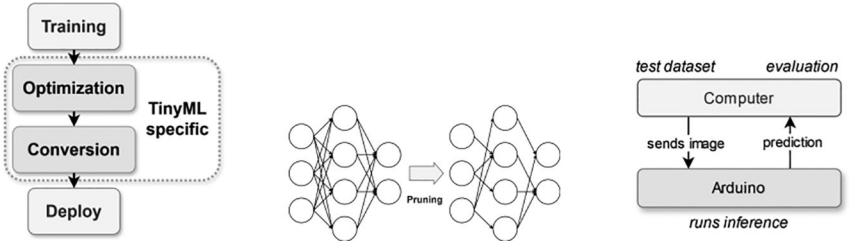


(a) Good weld (b) Lack of fusion (c) Contamination (d) Burn through

- The model training was conducted using TensorFlow, after which the model was converted to a TensorFlow Lite format to enable deployment on the microcontroller. Several optimization techniques were applied to ensure the model could operate within the limited memory, processing power, and energy consumption constraints of the microcontroller environment.

5. hardware's limitations:
   - Quantization: Converting model parameters to 8-bit integers to reduce memory usage.
   - Pruning: Eliminating low-weight connections in the neural network to further compress the model.

Fig. 4: The overall processes from model training to evaluation



(a) Model training (b) Optimization: Pruning (c) Evaluation on steps Arduino

6. Implementation and Evaluation:
   - The optimized model, which was reduced to 162 kB (11 times smaller than the baseline), was embedded into C++ code and executed using the Tensor-Flow Lite for Microcontrollers Interpreter. Due to the limited flash memory of the Arduino, test images were sent to the microcontroller one at a time via UART. The Arduino processed each image and returned a prediction.
   - The model achieved an impressive accuracy of 99% during evaluation. However, this high accuracy might be attributed to the similarity between the training and test data. Despite the microcontroller's limited resources, there was no significant loss in model accuracy, even after optimization.
   - One notable challenge was the inference time of approximately 800ms per image, which may be too slow for some real-time applications. This suggests that while TinyML is promising for low-cost and low-power applications, further optimization or more powerful hardware might be required for time-sensitive tasks.
7. Conclusion and Future Work: This project demonstrates the potential of TinyML in manufacturing, particularly in reducing the costs associated with quality control. The success of this implementation on a microcontroller like the Arduino Nano 33 indicates that TinyML could be a viable solution for small-scale manufacturers looking to integrate machine learning into their operations.

Future work should focus on deploying the model in a real production environment to assess its practical accuracy and robustness. Additionally, exploring the use of more powerful microcontrollers or further optimizing the model could help address the issue of slow inference times, making TinyML a more versatile tool for industrial applications.

4. Conclusion

The advancements in AI have significantly reshaped the manufacturing industry, driving improvements in efficiency, precision, and adaptability. Throughout this paper, we have explored various facets of AI-driven automation, including its applications predictive maintenance, and quality control. The potential of technologies such as TinyML, particularly in resource-constrained settings, was highlighted through a case study on a TinyML-based quality control solution. Additionally, the FESTO Cyber-Physical System demonstrated the real-world benefits of AI implementation in enhancing manufacturing processes. As manufacturing continues to evolve towards the Industry 4.0 framework, AI is expected to become even more integral, facilitating the development of interconnected, adaptive, and intelligent systems. These systems will not only enhance productivity but also contribute to greater sustainability and safety. However, challenges related to data availability, model optimization, and the creation of robust safety frameworks still need to be addressed. In summary, AI has emerged as a pivotal force in transforming manufacturing processes. Continued innovation, coupled with efforts to overcome current challenges, will ensure that AI-driven automation remains at the forefront of advancing the manufacturing industry in an increasingly competitive global landscape.

References

Abadade, Y., Temouden, A., Bamoumen, H., Benamar, N., Chtouki, Y., and Hafid, A. S. (2023). A comprehensive survey on tinyml. IEEE Access, 11:96892–96922.

Achouch, M., Dimitrova, M., Ziane, K., Sattarpanah Karganroudi, S., Dhouib, R., Ibrahim, H., and Adda, M. (2022). On predictive maintenance in industry 4.0: Overview, models, and challenges. Applied Sciences, 12(16):8081.

Akundi, A. and Reyna, M. (2021). A machine vision based automated quality control system for product dimensional analysis. Procedia Computer Science, 185:127–134.

Albanese, A., Nardello, M., Fiacco, G., and Brunelli, D. (2023). Tiny machine learning for high accuracy product quality inspection. IEEE Sensors Journal, 23(2):1575–1583.

Andreas Kornmaaler Hansen, L. C. and Lassen, A. H. (2024). Technology isn't enough for industry 4.0: on smes and hindrances to digital transformation. International Journal of Production Research, 0(0):1–21.

Ani, E. C., Olu-lawal, K. A., Olajiga, O. K., Montero, D. J. P., and Adeleke, A. K. (2024). Intelligent monitoring systems in manufacturing: current state and future perspectives. Engineering Science & Technology Journal, 5(3):750–759.

Arduino (2019). Arduino® nano 33 iot. https://docs.arduino.cc/resources/datasheets/ABX00027-datasheet.pdf.

Ayvaz, S. and Alpay, K. (2021). Predictive maintenance system for production lines in manufacturing: A machine learning approach using iot data in real-time. Expert Systems with Applications, 173:114598.

Bacioiu, D., Melton, G., Papaelias, M., and Shaw, R. (2019). Automated defect classification of aluminium 5083 tig welding using hdr camera and neural networks. Journal of manufacturing processes, 45:603–613.

Bai, H., Mou, S., Likhomanenko, T., Cinbis, R. G., Tuzel, O., Huang, P., Shan, J., Shi, J., and Cao, M. (2023). Vision datasets: A benchmark for vision-based industrial inspection.

Bommasani, R. et al. (2022). On the opportunities and risks of foundation models.

Carla Gon¸calves Machado, M. P. W. and da Silva, E. H. D. R. (2020). Sustainable manufacturing in industry 4.0: an emerging research agenda. International Journal of Production Research, 58(5):1462–1484.

Chan, F. T., Jiang, B., and Tang, N. K. (2000). The development of intelligent decision support tools to aid the design of flexible manufacturing systems. International journal of production economics, 65(1):73–84.

Chen, H., Chen, D., and Dai, H. (2021). Rdunet-a: A deep neural network method with attention for fabric defect segmentation based on autoencoder. In 2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID), pages 134–139. IEEE.

Chung, J., Gulcehre, C., Cho, K., and Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling.

coral.ai (2022). Coral dev board micro. https://coral.ai/products/dev-board-micro/f.

Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., and Fei-Fei, L. (2009). Imagenet: A large-scale hierarchical image database. In 2009 IEEE Conference on Computer Vision and Pattern Recognition, pages 248–255.

Ding, H., Gao, R. X., Isaksson, A. J., Landers, R. G., Parisini, T., and Yuan, Y. (2020). State of ai-based monitoring in smart manufacturing and introduction to focused section. IEEE/ASME Transactions on Mechatronics, 25(5):2143–2154.

Dutta, L. and Bharali, S. (2021). Tinyml meets iot: A comprehensive survey. Internet of Things, 16:100461.

Escobar, C. A. and Morales-Menendez, R. (2018). Machine learning techniques for quality control in high conformance manufacturing environment. Ad-vances in Mechanical Engineering, 10(2):1687814018755519.

Festo, F. D. (2021a). Cyber-physical systems. https://www.festo.com/net/en_corp/SupportPortal/Files/769597/CP%20Systems_Brochure_EN.pdf.

Festo, F. D. (2021b). Cyber-physical systems. https://www.festo.com/de/en/e/technical-education/training-concepts/highlights/training-factories/cp-systems-all-round-i4-0-training-factories/cp-lab-id_36133/.

Frank, A. G., Dalenogare, L. S., and Ayala, N. F. (2019). Industry 4.0 technolo-gies: Implementation patterns in manufacturing companies. International journal of production economics, 210:15–26.

Gheraibia, Y., Kabir, S., Aslansefat, K., Sorokos, I., and Papadopoulos, Y. (2019). Safety + ai: A novel approach to update safety models using artificial intelligence. IEEE Access, 7:135855–135869.

Ghobakhloo, M., Iranmanesh, M., Vilkas, M., Grybauskas, A., and Amran, A. (2022). Drivers and barriers of industry 4.0 technology adoption among manufacturing smes: a systematic review and transformation roadmap. Journal of Manufacturing Technology Management, 33.

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y. (2014). Generative adversarial networks.

Hata, A., Inam, R., Raizer, K., Wang, S., and Cao, E. (2019). Ai-based safety analysis for collaborative mobile robots. In 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pages 1722–1729.

He, K., Zhang, X., Ren, S., and Sun, J. (2015). Deep residual learning for image recognition.

Hearst, M., Dumais, S., Osuna, E., Platt, J., and Scholkopf, B. (1998). Support vector machines. IEEE Intelligent Systems and their Applications, 13(4):18–28.

Huang, G., Liu, Z., van der Maaten, L., and Weinberger, K. Q. (2018). Densely connected convolutional networks.

Huang, T. S. (1996). Computer vision: Evolution and promise.

Jaeger, B. and Upadhyay, A. (2020). Understanding barriers to circular economy: cases from the manufacturing industry. Journal of Enterprise Information Management, 33(4):729–745.

Javaid, M., Haleem, A., Singh, R. P., and Suman, R. (2022). Artificial intelligence applications for industry 4.0: A literature-based study. Journal of Industrial Integration and Management, 7(01):83–111.

Judi, H. M., Genasan, D., and Jenal, R. (2011). Quality control implementation in manufacturing companies: motivating factors and challenges. INTECH Open Access Publisher.

Kallimani, R., Pai, K., Raghuwanshi, P., Iyer, S., & López, O. L. (2024). TinyML: Tools, applications, challenges, and future research directions. Multimedia Tools and Applications, 83(10), 29015–29045.

Kempf, K. G. (1985). Manufacturing and artificial intelligence. Robotics, 1(1):13–25.

Klingenberg, C. (2017). Industry 4.0: what makes it a revolution?

Kovács, G. L. (1997). Ai in manufacturing: application to fms simulation, scheduling and control. In Computer-Assisted Management and Control of Manufacturing Systems, pages 83–117. Springer.

Kovalenko, I., Barton, K., Moyne, J., and Tilbury, D. M. (2023). Opportunities and challenges to integrate artificial intelligence into manufacturing systems: Thoughts from a panel discussion [opinion]. IEEE Robotics & Automation Magazine, 30(2):109–112.

Krizhevsky, A., Sutskever, I., and Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In Pereira, F., Burges, C., Bottou, L., and Weinberger, K., editors, Advances in Neural Information Processing Systems, volume 25. Curran Associates, Inc.

Lakshman, S. B. and Eisty, N. U. (2022). Software engineering approaches for tinyml based iot embedded vision: A systematic literature review. In Pro-ceedings of the 4th International Workshop on Software Engineering Re-search and Practice for the IoT, pages 33–40.

LeCun, Y., Bengio, Y., and Hinton, G. (2015). Deep learning. nature, 521(7553): 436–444.

LeCun, Y., Bottou, L., Bengio, Y., and Haffner, P. (1998). Gradient-based learning applied to document recognition. Proc. IEEE, 86:2278–2324.

Leyendecker, L., Agarwal, S., Werner, T., Motz, M., and Schmitt, R. H. (2023). A study on data augmentation techniques for visual defect detection in manufacturing. In Lohweg, V., editor, Bildverarbeitung in der Automation, pages 73–94, Berlin, Heidelberg. Springer Berlin Heidelberg.

Liu, L. and Du, K. (2024). A perspective on computer vision in biosensing. Biomicrofluidics, 18.

McCarthy, J., Minsky, M., Rochester, N., and Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. AI Mag., 27:12–14.

McDermid, J., Jia, Y., and Habli, I. (2019). Towards a framework for safety assurance of autonomous systems.

Minsky, M. and Papert, S. (1969). Perceptrons: An Introduction to Computational Geometry. MIT Press, Cambridge, MA, USA.

Mypati, O., Mukherjee, A., Mishra, D., Pal, S. K., Chakrabarti, P. P., and Pal, A. (2023). A critical review on applications of artificial intelligence in manufacturing. Artificial Intelligence Review, 56(Suppl 1):661–768.

OpenAI (2023). Chatgpt: Openai's gpt-4. Available at https://openai.com/.

Papert, S. (1966). The summer vision project.

Parunak, H. V. D. (1996). Applications of distributed artificial intelligence in industry. Foundations of distributed artificial intelligence, 2(1):18.

Plathottam, S. J., Rzonca, A., Lakhnori, R., and Iloeje, C. O. (2023). A review of artificial intelligence applications in manufacturing operations. Journal of Advanced Manufacturing and Processing, 5(3):e10159.

Quinlan, J. R. (1986). Induction of decision trees. Machine Learning, 1:81–106. Rabelo, L. C. and Alptekin, S. (1989). Integrating scheduling and control functions in computer integrated manufacturing using artificial intelligence. Computers & industrial engineering, 17(1–4):101–106.

Rawat, W. and Wang, Z. (2017). Deep convolutional neural networks for image classification: A comprehensive review. Neural Computation, 29:1–98.

Roberts, L. G. (1963). Machine perception of three-dimensional solids. In Outstanding Dissertations in the Computer Sciences.

Rodríguez-Somoza, B., Galán, R., and Puente, E. (1990). Production scheduling using ai techniques. In Information Control Problems in Manufacturing Technology 1989, pages 387–392. Elsevier.

Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage and organization in the brain. Psychological Review, 65(6):386–408.

Rumelhart, D. E., Hinton, G. E., and Williams, R. J. (1986). Learning representations by back-propagating errors. Nature, 323:533–536.

Ryabchik, T. A., Smirnova, E. E., Lukashova, M. I., and Haydar, H. (2019). Manufacturing processes quality control as a main factor of performance enhancement in industrial management. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pages 1463–1466.

Sampath, V., Maurtua, I., Aguilar Martin, J. J., and Gutierrez, A. (2021). A survey on generative adversarial networks for imbalance problems in computer vision tasks. Journal of big Data, 8:1–59.

Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. IBM Journal of Research and Development, 3(3):210–229.

Sezer, E., Romero, D., Guedea, F., Macchi, M., and Emmanouilidis, C. (2018). An industry 4.0-enabled low cost predictive maintenance approach for smes. In 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), pages 1–8.

Sharma, H. and Kumar, H. (2024). A computer vision-based system for real-time component identification from waste printed circuit boards. Journal of Environmental Management, 351:119779.

Simonyan, K. and Zisserman, A. (2015). Very deep convolutional networks for large-scale image recognition.

Systems, E. (2023). Esp32-s3-eye. https://www.espressif.com/sites/default/files/documentation/esp32-s3-wroom-1_wroom-1u_ datasheet_en.pdf.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., and Rabinovich, A. (2014). Going deeper with convolutions.

Szeliski, R. (2010). Computer Vision: Algorithms and Applications. Texts in Computer Science. Springer London.

Toosi, A., Bottino, A. G., Saboury, B., Siegel, E., and Rahmim, A. (2021). A brief history of ai: How to prevent another winter (a critical review). PET Clinics, 16(4):449–469.

Turing, A. M. (1950). Computing machinery and intelligence. Mind, 59 (October):433–60.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L. u., and Polosukhin, I. (2017). Attention is all you need. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R., editors, Advances in Neural Information Processing Systems, volume 30. Curran Associates, Inc.

Wan, J., Li, X., Dai, H.-N., Kusiak, A., Martinez-Garcia, M., and Li, D. (2020). Artificial-intelligence-driven customized manufacturing factory: key technologies, applications, and challenges. Proceedings of the IEEE, 109(4):377–398.

Wang, B. (2018). The future of manufacturing: A new perspective. Engineering, 4(5):722–728.

Warden, P. and Situnayake, D. (2019). Tinyml: Machine learning with tensorflow lite on arduino and ultra-low-power microcontrollers. O'Reilly Media.

Xia, C., Pan, Z., Fei, Z., Zhang, S., and Li, H. (2020). Vision based defects detection for keyhole tig welding using deep learning with visual explanation. Journal of manufacturing processes, 56:845–855.

Xu, J., Kovatsch, M., Mattern, D., Mazza, F., Harasic, M., Paschke, A., and Lucia, S. (2022). A review on ai for smart manufacturing: Deep learning challenges and solutions. Applied Sciences, 12(16):8239.

Zhang, H.-C. and Huang, S. (1995). Applications of neural networks in manufacturing: a state-of-the-art survey. The International Journal of Production Research, 33(3):705–728.

Zheng, Y., Mao, S., Liu, S., Wong, D. S.-H., and Wang, Y.-W. (2016). Normalized relative rbc-based minimum risk bayesian decision approach for fault diagnosis of industrial process. IEEE Transactions on Industrial Electronics, 63(12):7723–7732.

Zonta, T., Da Costa, C. A., da Rosa Righi, R., de Lima, M. J., da Trindade, E. S., and Li, G. P. (2020). Predictive maintenance in the industry 4.0: A system-atic literature review. Computers & Industrial Engineering, 150:106889.

Iryna Piatnychuk, Valentyna Yakubiv, Liliia Turovska,
Iryna Hryhoruk*

Problems and Trends of the Youth Labor Market: Case Poland and Ukraine

Abstract: The article examines the main problematic issues of the labor market for young people and the search for ways to solve them. It has been determined what skills young people need for employment and career growth. The main trends in the labor market in Poland and the Polish experience in solving the current situation were studied; compared the analysis of recent years on the labor markets of Ukraine and Poland; the experience of Poland as one of the EU countries in this direction is studied. In addition, it was investigated how dual education affects labor market trends. The obtained results will be valuable for young people, as they will help to understand the demands placed on them. They will also be valuable for educational institutions, as they will allow the development of educational programs that will be useful for young people, taking into account the demands of the market.

Keywords: youth labor market, digital skills, dual education, public administration, public administration of higher education, mechanisms of public administration, experience of EU countries

1. Introduction

Poland is one of the 27 EU member states in 2020, with an employment rate of 73.6% in the 20–64 age group. In 2021, this figure increased to 75.4%, compared to the EU average of 73.1% (European Commission, 2023). Overall, the key indicators describing the labor market situation in Poland improved every year. Positive growth trends slowed in 2020 due to the COVID-19 pandemic and the restrictions imposed on economies as a result. However, contrary to fears of an anticipated labor market crisis, there was only a slowdown in the growth of key indicators.

The purpose of the article is to explore the challenges and trends of the youth labor market using the example of Poland, which can be used for Ukraine.

The objectives of the article are: - To study labor market trends in Poland and the Polish experience in solving problematic issues;

* *Vasyl Stefanyk Precarpathian National University*

- To examine Poland's experience as one of the EU countries in addressing labor market problems;
- To identify the skills needed by young people for employment and career growth in Ukraine;
- To investigate how dual education affects labor market trends in Ukraine.

2. The state of the Polish labor market

To diagnose the state of the labor market in Poland, it is considered appropriate, first of all, to analyze the information on the number of jobs in Poland from 2019 to 2023, which is presented in Table 1. The data for the analysis was obtained from the Statista website.

Table 1: Analysis of information on the number of jobs in Poland from 2019 to 2023 (in thousands)

Quarter	2019	2020	2021	2022	2023	Absolute deviation, +,-				Relative deviation, %			
						2023/ 2019	2023/ 2020	2023/ 2021	2023/ 2022	2023/ 2019	2023/ 2020	2023/ 2021	2023/ 2022
Quarter 1	142,50	76,50	110,20	158,70	114,90	–27,60	+38,40	+4,70	–43,80	–19,37	+50,20	+4,26	–27,60
Quarter 2	151,80	81,40	142,80	149,30	113,20	–38,60	+31,80	–29,60	–36,10	–25,43	+39,07	–20,73	–24,18
Quarter 3	148,60	91,10	153,50	135,50	111,20	–37,40	+20,10	–42,30	–24,30	–25,17	+22,06	–27,56	–17,93
Quarter 4	125,40	84,40	137,40	115,70	97,10	–28,30	+12,70	–40,30	–18,60	–22,57	+15,05	–29,33	–16,08

Source: https://www.statista.com/topics/9022/employment-in-poland/

As a result of the study on the number of jobs in Poland by quarter from 2019 to 2023, it was found that there has been a decreasing trend in the number of jobs across all quarters since 2019, with the number of jobs decreasing in 2023.

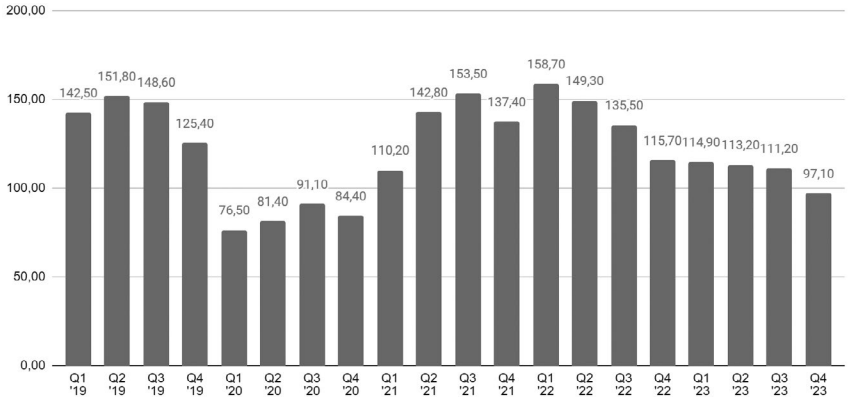
For example, in the first quarter of 2023, the number of jobs was 114.9 thousand, which decreased by 43.8 thousand, or 27.6%, compared to the corresponding quarter of 2022. Compared to the first quarter of 2019, it decreased by 27.6 thousand, or 19.37%, which should be considered a significant fluctuation. However, when comparing the first quarter of 2023 with the corresponding quarters of 2020 and 2021, there was an increase in the number of vacancies by 38.4 thousand (50.2%) and 4.7 thousand (4.26%), respectively, due to the COVID-19 pandemic and the reduction in the number of jobs related to lockdowns.

In the second quarter of 2023, the number of jobs was 113.2 thousand, which decreased by 36.1 thousand, or 24.18%, compared to the corresponding quarter of 2022. Compared to the first quarter of 2021, it decreased by 29.6 thousand, or 20.73%. When compared to the first quarter of 2019, it decreased by 38.6

thousand, or 25.43%. Comparing the first quarter of 2023 with the corresponding quarter of 2020, there was an increase in the number of jobs by 31.8 thousand (or 39.07%).

The overall trend in the number of jobs in Poland from 2019 to 2023 can be seen in Fig. 1.

Fig. 1: Number of jobs in Poland from 2019 to 2023 (in 1,000)



Source: https://www.statista.com/topics/9022/employment-in-poland/

In the third quarter of 2023, the number of jobs was 111.2 thousand, which decreased by 24.3 thousand, or 17.93%, compared to the corresponding quarter of 2022, and decreased by 42.3 thousand, or 27.56%, compared to the first quarter of 2021. Compared to the first quarter of 2019, it decreased by 37.4 thousand, or 25.30%. When comparing the first quarter of 2023 with the corresponding quarter of 2020, there was an increase in the number of jobs by 20.1 thousand (or 22.06%).

In the fourth quarter of 2023, the number of jobs was 97.1 thousand (the lowest for all of 2023), which decreased by 18.6 thousand, or 16.08%, compared to the corresponding quarter of 2022, and decreased by 40.3 thousand, or 29.33%, compared to the first quarter of 2021. Compared to the first quarter of 2019, it decreased by 28.3 thousand, or 22.57%. When comparing the first quarter of 2023 with the corresponding quarter of 2020, there was an increase in the number of jobs by 12.7 thousand (or 15.05%).

A significant decrease in the number of jobs was observed in 2020 across all quarters, which was due to the COVID-19 pandemic and lockdowns. The number of jobs in 2020 ranged from 76.5 to 91.0 thousand.

In the process of analyzing the number of jobs, it is necessary to analyze the number of vacancies in Poland from 2009 to 2024 (Table 2), which were obtained from the Statista website.

Table 2: Analysis of information on the number of vacancies in Poland from 2009 to 2024

Year	Number of vacancies, thousand	Compared to the previous year, +, –	Compared to the previous year, %
2009	51,6	–	–
2010	58,9	+7,3	+14,15
2011	45,5	–13,4	–22,75
2012	35,5	–10	–21,98
2013	39,2	+3,7	+10,42
2014	54,4	+15,2	+38,78
2015	63,9	+9,5	+17,46
2016	78	+14,1	+22,07
2017	117,8	+39,8	+51,03
2018	139,2	+21,4	+18,17
2019	125,4	–13,8	–9,91
2020	84,4	–41	–32,70
2021	137,4	+53	+62,80
2022	115,7	–21,7	–15,79
2023	97,1	–18,6	–16,08
2024	111,3	+14,2	+14,62

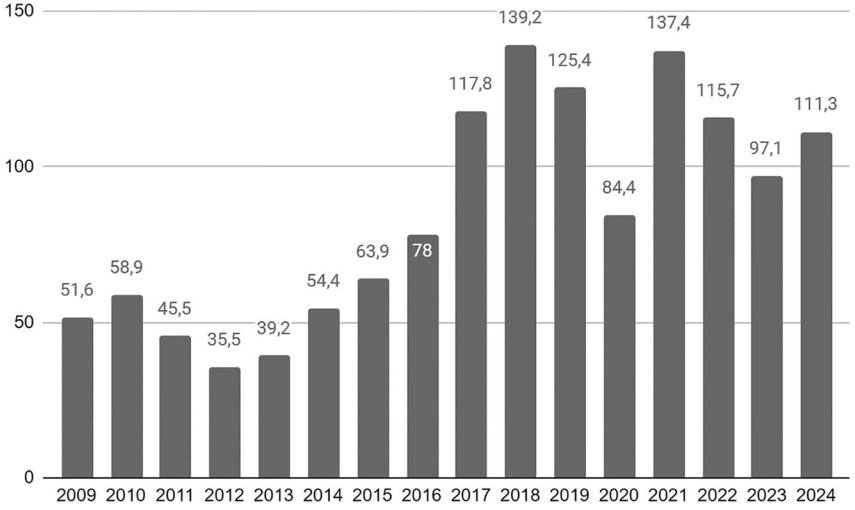
Source: https://www.statista.com/topics/9022/employment-in-poland/

As a result of the analysis, it was found that during the analyzed period, the highest number of vacancies in Poland was in 2018, with 139.2 thousand vacancies, and the lowest was in 2012, with 35.5 thousand vacancies (Fig. 2).

It was found that during the analyzed period, the number of vacancies among Polish employers increased the most in 2021 compared to the previous year (2020) by 53 thousand positions, or 62.8%. The largest decrease (decline) occurred in 2020 compared to the previous year, 2019, by 41 thousand positions, or 32.7%.

To compare the information on the number of vacancies in Poland with other EU member countries, an analysis was conducted, which is presented in Table 3.

Fig. 2: Number of vacancies in Poland 2009–2023, thousands



Source: https://www.statista.com/topics/9022/employment-in-poland/

Table 3: Number of vacancies in selected EU countries in July 2024, in thousands

Country	Last	Previous	Absolute deviation, +, –	Relative deviation, %
Germany	1326,52	1555,93	–229,41	–14,74
Netherlands	415,00	409,60	+5,40	+1,32
Belgium	185,28	184,43	+0,84	+0,46
Austria	174,72	196,44	–21,73	–11,06
Sweden	150,88	108,37	+42,50	+39,22
Spain	144,29	146,99	–2,71	–1,84
Poland	111,31	96,60	+14,71	+15,23
Hungary	69,32	73,79	–4,48	–6,07
Finland	59,46	41,74	+17,71	+42,43
Portugal	48,25	49,35	–1,10	–2,22
Romania	34,02	34,59	–0,58	–1,67
Lithuania	27,22	25,76	+1,46	+5,66
Croatia	24,92	17,55	+7,37	+42,00

(*Continued*)

Table 3: (Continued)

Country	Last	Previous	Absolute deviation, +, –	Relative deviation, %
Ireland	24,70	24,70	0,00	0,00
Latvia	24,22	22,23	+1,99	+8,97
Slovenia	20,60	20,94	–0,34	–1,64
Bulgaria	17,46	15,54	+1,92	+12,36
Estonia	11,45	7,84	+3,61	+46,04
Luxembourg	7,28	7,47	–0,19	–2,51

Source: https://www.statista.com/topics/9022/employment-in-poland/

As a result of the analysis, it was found that according to Eurostat data in July 2024, Germany had the highest number of vacancies among the EU member countries - 1,326.52 thousand - followed by the Netherlands with 415.0 thousand, and Belgium with 185.28 thousand. As previously mentioned, Poland had 111.31 thousand vacancies, an increase of 14.41 thousand positions, or 15.23%, compared to the same period of the previous year. Luxembourg had the lowest number of vacancies among the listed countries, with 7.28 thousand.

Research conducted by the Central Statistical Office shows that despite an increase in the unemployment rate in Poland to 5.4%, the country still has one of the lowest unemployment rates in the European Union. However, Polish employers report a growing need to hire new workers. The current number of vacancies indicates a dynamic labor market full of opportunities for job seekers.

It was found that the highest demand for workers is in the following sectors: IT industry workers, production workers, simple industrial laborers, domestic workers, office workers, and warehouse workers (Worktime, 2024).

It is also considered appropriate to study the monthly unemployment rate in Poland. In June 2024, the unemployment rate in Poland was 4.9%, which was lower than a year earlier when it reached 5.1%. According to the Central Statistical Office, the number of job offers submitted to employment services has slightly increased.

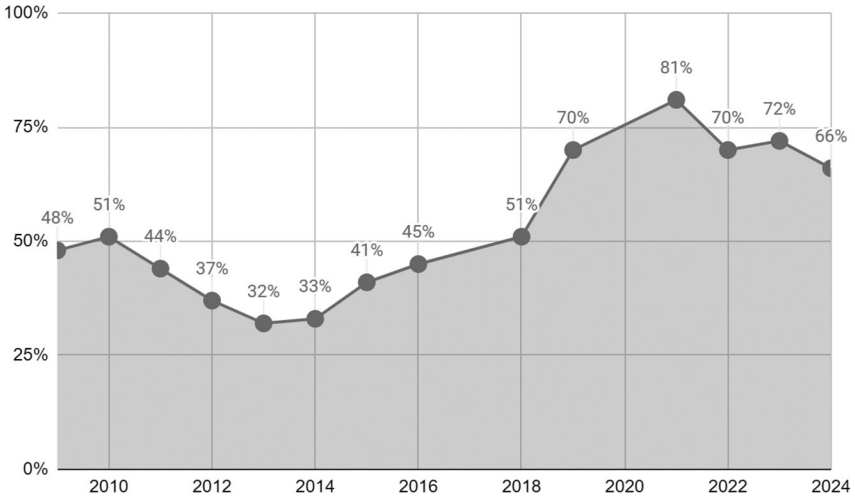
Regarding the characteristics of the unemployed in Poland, it is worth noting that at the end of 2022, the number of unemployed Poles reached 812.3 thousand. Between 2009 and 2022, the number of unemployed Poles with incomplete secondary and primary education decreased. However, they still remain the

largest group among the unemployed in the country. Unemployment is more severe among young people. In 2022, the age groups 25–34 and 35–44 led and shared the same figures - about 200 thousand unemployed each. Considering gender, there were 61 thousand more registered unemployed women than men in Poland.

When analyzing job offers and requirements in Poland, it was found that in June 2023, the number of monthly job offers submitted to employment services slightly increased, resulting in better prospects for unemployed Poles. In contrast, in 2022, there were over 115 thousand vacancies and 89 thousand newly created jobs. According to online job platforms, in 2020, all requirements for candidates were somewhat lowered due to the coronavirus (COVID-19) epidemic. However, one of the most necessary skills for employment in Poland was experience. The next requirement for applying for jobs on online platforms was education (Simply Talented, 2024).

Another important issue in the labor market is the talent shortage in Poland, which we studied for the period 2009–2024 and presented in Fig. 3. It should be noted that the greatest shortage during the analyzed period was observed in 2021 at 81%, while the lowest was in 2013 at 32%. In 2024, the talent shortage rate in Poland stands at 66%, which is quite high and indicates a strong demand from employers for highly skilled and talented workers.

Fig. 3: Talent shortage in Poland from 2009 to 2024



Source: https://www.statista.com/topics/9022/employment-in-poland/

To compare the state of the labor market, it is considered appropriate to study the information on the unemployment rate in Ukraine from 2009 to 2024, as presented in Table 4, which is compiled based on data from the Ministry of Finance of Ukraine (Minfin, 2024).

From the information provided in the table, we can note that the unemployment rate in 2024 is 18.1%. During the analyzed period, the highest unemployment rate was in 2022, at 21.1%, and the lowest was in 2013, at 7.7%. It is worth noting that the State Statistics Service of Ukraine has not provided labor market data since 2022 due to the war in Ukraine.

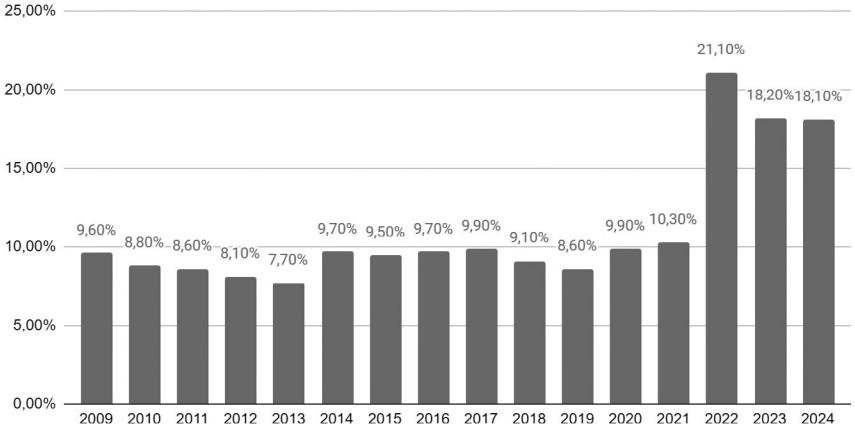
Table 4: Unemployment rate in Ukraine from 2009 to 2024

Year	Total population	Registered unemployed	Unemployment rate	Change in the unemployment rate compared to the previous year, %
2009	45982,9	693,1	9,60%	–
2010	45795,9	452,1	8,80%	–0,80%
2011	45644,4	505,3	8,60%	–0,20%
2012	45560,3	467,7	8,10%	–0,50%
2013	45439,8	487,6	7,70%	–0,40%
2014	42953,9	458,6	9,70%	+2,00%
2015	42774,6	461,1	9,50%	–0,20%
2016	42603,9	407,2	9,70%	+0,20%
2017	42403,0	352,5	9,90%	+0,20%
2018	42177,6	341,7	9,10%	–0,80%
2019	41922,7	338,2	8,60%	–0,50%
2020	41629,9	459,2	9,90%	+1,30%
2021	41208,1	295,0	10,30%	+0,40%
2022	41167,3	186,5	21,10%	+10,80%
2023	н/д	96,1	18,20%	–2,90%
2024	н/д	106,7	18,10%	–0,10%

Source: https://www.statista.com/topics/9022/employment-in-poland/

The general trend regarding the level of unemployment in Ukraine for 2009–2024 can be seen in Fig. 4.

Fig. 4: Unemployment rate in Ukraine for 2009–2024



Source: https://index.minfin.com.ua/ua/labour/unemploy/register/

Based on the research conducted, the following key issues currently exist in the labor market in Ukraine (EBA, 2024): talent shortage; mobilization; preference for remote work; outflow of skilled workers abroad; employee burnout and fatigue; reluctance of recruiters and employers to collaborate with candidates aged 40+; low level of inclusivity and few initiatives to engage veterans and people with disabilities; lack of strategic management of demographic processes; students going abroad for education; internal redistribution of the workforce (concentration of candidates in safer regions); Ukrainian businesses continuing to operate in the "grey" or "black" market, which does not attract the return of emigrated population; disparities between candidates' salary expectations and the financial capabilities of businesses; lack of specialists with English language proficiency; official employment of those liable for military service (due to the risk of being mobilized).

For comparison, it is considered appropriate to study the information on the number of vacancies in Ukraine (according to data from the most popular job search website Work.ua, 2024), as presented in Table 5.

Based on the data presented in the table, we can note that in 2024, the number of vacancies amounted to 4,500.44 thousand, and compared to the previous year, it increased by 170.19 thousand vacancies, or by 3.93%. It is worth noting that due to the war in Ukraine and for reasons of national security, a significant amount of statistical data is not officially published in Ukraine, making it difficult to compare certain labor market indicators at this time.

Table 5: Number of vacancies in Ukraine, in thousands

Year	Number of vacancies, thousand	Compared to the previous year, +,–	Compared to the previous year, %
2021	3385,89	–	–
2022	3996,06	+610,17	+18,02
2023	4330,25	+334,19	+8,36
2024	4500,44	+170,19	+3,93

Source: https://www.work.ua/

3. Tools to Support Youth in Poland

It should be noted that youth employment in Poland is supported by a range of services and tools provided by the country's legislation. Many services and tools designed for young people are implemented through public labor market institutions - Employment Offices and the Voluntary Labor Corps. It has been established that during the early decades of the market economy, the unemployment rate among young people was very high. After 2015, the youth unemployment rate in Poland began to decrease.

At Employment Offices, individuals can use the following support tools: job search, employment services; public and socially beneficial work, reimbursement of travel and accommodation expenses, reimbursement of child care expenses for children under 7 years; skill enhancement: internships, training, tripartite training agreements, adult internships, scholarships for continuing education, educational loans; co-founding and lending for entrepreneurial activities; job vouchers, housing vouchers, internship vouchers, training vouchers; reimbursement of social insurance contributions for unemployed persons under 30 who are employed for the first time (valid for 12 months, after which the employer must employ the person for another 6 months).

As a result of these programs, in 2019, the number of unemployed people who utilized the labor market increased. The largest number of unemployed persons under 30 began internships - 60.7 thousand people - and began training - 17.1 thousand people. As a result of the introduction of such tools as training vouchers, internship vouchers, employment vouchers, or job vouchers, approximately 105,000 young people under 30 were activated between 2014 and 2019 (European Commission, 2023).

Another factor that has helped improve the labor market situation is the implementation of the Youth Guarantee Initiative, which was launched in Poland in 2014. Four subgroups of individuals have been identified as targets of the Youth Guarantee Initiative:

- Persons aged 15 to 17 who leave school early or neglect their education obligations;
- Persons aged 18 to 29 who are not in employment, education, or training, including those in need of special support;
- Persons aged 18 to 29 registered as unemployed, including registered students in part-time and evening programs;
- Unemployed youth and those employed within 48 months of graduation from secondary and higher education institutions, aged 18 to 29.

Over the period of the Youth Guarantee Initiative's implementation, more than 4.3 million young people have been covered, of whom 2.7 million were employed, underwent training, professional preparation, and internships (European Commission, 2023).

Since 2014, a credit program for youth has been implemented, provided by the National Development Bank. It is now a government program called "First Business - Start-up Support".

In addition to the aforementioned services, Employment Offices, in cooperation with other institutions, implement projects that provide individual psychological support; group active job search workshops; professional courses; professional qualification courses; language courses; driving courses; entrepreneurship courses; employment and mediation in organizing internships; and internships with employers. The goal of the projects is to activate people aged 18–24 from the group.

The EU Council's "Reinforcing the Youth Guarantee" recommendation of October 2020 focuses more on developing participants' digital skills within the program's activation activities. Thus, it is expected that any candidate interested in participating will be able to undergo an assessment of their existing skills at the outset and, if deficiencies are identified, will have the opportunity to correct them by participating in a training course to improve digital skills. The financial source will be the European Social Fund (ESF).

The new edition of the "Youth Guarantee" (2022) targets young people in four subgroups (European Commission, 2023):

- Ages 15–17 who drop out of school or neglect compulsory education;
- Individuals aged 18–29: registered as unemployed; those who are not in employment, education, or training; those who are unemployed and university graduates;
- Those who have left foster care;
- Women under the age of 30 who are raising children.

The key institutions implementing measures to support youth entering the labor market are: district and provincial labor offices; Voluntary Labor Corps; the Bank of National Economy, among others.

In 2022, PFRON launched a new program, "Independence-Activity-Mobility", Housing for Graduates (2022). This is a subsidy for renting an apartment or house for a period of job search and initial employment for up to 36 months.

4. Skills Needed for Youth Employment and Career Growth

An important factor in the effectiveness of public administration of higher education and youth employment is having the relevant skills. According to a study conducted by the European Business Association (EBA, 2024) on the skills needed in 2024–2025, the following were highlighted: stress management and resilience; self-organization; adaptability and flexibility; emotional intelligence; humanity; willingness to learn; knowledge of foreign languages; working with new technologies and AI; critical thinking; effective communication; and change management.

For employment and career growth in Poland and Ukraine, young people need a variety of skills. Based on the results of the study, the following skills were identified for youth employment in Poland:

1. Knowledge of the Polish language. For many vacancies, especially in service, sales, and administration sectors, knowledge of the Polish language is essential. English is also appreciated, especially in international companies.
2. Technical skills. IT, engineering, and technology sectors require highly qualified specialists in programming, software development, web design, and other technical specializations.
3. Soft skills. Employers value communication skills, teamwork ability, flexibility, adaptability, leadership qualities, and critical thinking.
4. Professional experience and qualifications. Practical work experience, certificates, and other professional qualifications are important, especially for positions in medicine, finance, and project management.
5. Digital skills. As digitalization accelerates, employers are looking for workers with computer skills, knowledge of basic software packages (Microsoft Office, Google Workspace), and understanding of social media.

Considering the above, we have grouped the skills that youth should possess for employment in Ukraine and identified the following:

1. Knowledge of Ukrainian and English languages. In most fields, knowledge of the Ukrainian language is mandatory. English is increasingly valued, especially in international companies or companies focused on export.

2. Technical skills. The IT sector in Ukraine is very developed, so knowledge of programming, cybersecurity, data analysis, DevOps, and other specialized technical skills is a significant advantage.
3. Soft skills. Employers value communication skills, adaptability, problem-solving skills, leadership, and the ability to work in a team.
4. Professional experience and qualifications. Work experience in a specific field, especially in finance, law, medicine, and engineering, is important. Certifications, internships, and additional education are also welcomed.
5. Entrepreneurial skills. Given economic instability, many young people in Ukraine are considering starting their own business, which requires knowledge in management, marketing, sales, and finance.

It is advisable to compare these groups of skills:

- Language: In both countries, language knowledge is critical, but in Poland, there is a special emphasis on the Polish language, while in Ukraine, Ukrainian is mandatory, and English is often an advantage;
- Technical skills: There is high demand for technical professions in both countries, particularly in the IT sector. However, in Poland, there is also a demand for engineers and specialists in manufacturing;
- Soft skills: Soft skills are valued in both Poland and Ukraine, but in the context of globalization and constant changes, these skills are becoming increasingly important in both countries;
- Professional qualifications: In both countries, work experience and professional certifications are significant for career growth. In Poland, more attention is paid to professional experience in specific fields, such as medicine and finance, while in Ukraine, young people often focus on IT and entrepreneurship;
- Digital skills: In both Poland and Ukraine, employers value knowledge of digital tools, but in Ukraine, particular attention is given to skills related to online promotion and marketing, given the development of the digital economy.

Thus, for successful employment and career growth, young people should adapt their skills to the labor market requirements of a particular country, considering local specifics and global trends.

5. The Impact of Dual Education on Labor Market Trends

Our research shows that dual education, which combines classroom learning with practical training in the workplace, has a significant impact on labor market trends. This education system allows students to gain not only theoretical knowledge but also practical skills that meet employers' needs. Here are some

public administration mechanisms for higher education regarding the use of dual education and its impact on the labor market:

1. Improving the quality of specialist training. Dual education promotes better training of specialists, as students gain practical experience directly in enterprises. This allows graduates to be better prepared for real working conditions and adapt more quickly to employers' requirements. As a result, employers receive qualified workers who possess not only theoretical knowledge but also practical skills, reducing the need for extended additional training.
2. Reducing youth unemployment. Since dual education is closely linked to the actual needs of the labor market, graduates of such programs have a higher chance of employment. Many companies are willing to hire students during their studies, which helps reduce youth unemployment and facilitates better integration of graduates into the labor market.
3. Adapting to rapid changes in the labor market. Dual education provides flexibility in the learning process, as programs can quickly adapt to changes in the labor market. This is especially important in the context of rapid technological development and globalization, where employers' needs change rapidly. Educational institutions within dual education can promptly update their curricula to meet new requirements.
4. Strengthening cooperation between educational institutions and businesses. Dual education promotes strengthening cooperation between educational institutions and companies. This partnership allows businesses to actively participate in developing curricula, provide internships and training programs for students, and help develop the necessary skills in future workers. Such cooperation can also lead to the emergence of new industries and specializations that meet modern market requirements.
5. Developing entrepreneurial skills. Students participating in dual education can acquire not only technical skills but also develop entrepreneurial skills such as time management, teamwork, leadership, critical thinking, and problem-solving. This makes them more competitive in the labor market and prepares them for potentially starting their own business.
6. Reducing the Gap Between Education and the Labor Market. The dual education system helps reduce the gap between theoretical training and the real requirements of the labor market. This prevents situations where graduates lack the necessary skills or knowledge for specific jobs. Thus, dual education ensures a more harmonious development of the labor market, where graduates are prepared for modern challenges and can quickly integrate into the workforce.

7. Development of the Local Economy. By training qualified specialists who meet the local labor market needs, dual education contributes to the development of the local economy. Local businesses receive employees who are already familiar with the specifics of the work and are ready to be effective from day one.

Therefore, it has been established that dual education significantly impacts labor market trends by promoting the training of qualified specialists, reducing youth unemployment, adapting to rapid labor market changes, strengthening cooperation between business and education, and developing the local economy. This education model helps better prepare young people for the demands of the modern labor market and contributes to the formation of a flexible and competitive workforce.

6. Conclusions

The analysis highlights critical issues in the youth labor markets of Poland and Ukraine, identifying the essential skills young people need to secure employment and thrive in their careers. The study demonstrates Poland's success in addressing labor market challenges, offering valuable insights for Ukraine as it seeks to align with EU labor standards. Comparative analysis of recent labor market trends in both countries underscores the need for continuous adaptation of youth skillsets to meet changing job demands, with dual education emerging as an influential factor in bridging the skills gap.

Based on these findings, educational institutions in Ukraine and Poland could benefit from aligning their curricula with market requirements, equipping students with practical skills that improve their employability. This might include expanding dual education programs and fostering partnerships between educational institutions and employers to better integrate theoretical and practical knowledge.

However, several questions remain open for further research. Future studies could explore how specific dual education models impact youth employability across different industries. Additionally, there is a need to investigate the long-term career trajectories of youth participating in these programs to understand their effectiveness fully. Finally, examining the role of digital skills in enhancing youth employment opportunities would offer valuable insights as labor markets continue to evolve.

References

Employment in Poland - statistics & facts. 2024. Statista. Retrieved from https://www.statista.com/.

Level of unemployment in Poland in 2024. 2024. Worktime. Retrieved from https://worktimeeu.com/en/level-of-unemloyment-in-poland-in-2024/.

Kilkist zareiestrovanykh bezrobitnykh [Number of registered unemployed]. 2024. Minfin. Retrieved from https://index.minfin.com.ua/ua/labour/unemploy/register/.

Try chverti robotodavtsiv vidchuvaiut defitsyt kadriv v Ukraini [Three quarters of employers experience a shortage of personnel in Ukraine]. 2024. Eba. Retrieved from https://eba.com.ua/try-chverti-robotodavtsiv-vidchuvayut-defitsyt-kadriv-v-ukrayini/.

Kilkist vakansii v Ukraini [The number of vacancies in Ukraine]. 2024. Work.ua. Retrieved from https://www.work.ua/.

The job market in Poland and globally for the year 2024 analysis and challenges. 2024. Simply Talented. Retrieved from https://wearesimplytalented.com/the-job-market-in-poland-and-globally-for-the-year-2024-analysis-and-challenges/.

Labour market information: Poland. 2023. European Commision. Retrieved from https://eures.europa.eu/living-and-working/labour-market-information/labour-market-information-poland_en.

Dominika Liszkowska*

The Use of Modern Technological Tools and the Internet in Creating an Image and Personal Brand

Abstract: Modern technologies have become a very useful tool for promoting ideas and values that are an elementary part of social and public life. Currently, for almost every user, the Internet has become a platform for dialogue, information exchange, and opinion creation. Every entity (person, company, or institution) actively operating in public space today must consider how to present on the Internet, including the issue of image creation. Conducting campaigns focused on Internet tools is currently a necessary condition for a positive result in building a personal brand in many spheres of social life.

Due to the fact that the Internet is a very dynamically changing space, on the one hand, it constantly poses new challenges for users. On the other hand, it provides new tools for reaching audiences, generating the need to constantly adapt to the conditions of the online community. This chapter aims to show the importance of the Internet and the ability to use modern technologies to create one's own image. It was important to present the key principles and strategies for building a personal brand in cyberspace and the effectiveness factors of social media used for this purpose.

Keywords: Image, Personal Brand, Persona Branding, Internet, Social Media

Introduction

The development of new media is a continuous process that enters numerous areas related to both the transfer of information and broadly understood communication, as well as the economic and social sphere. The emergence of new forms of contact, and their dynamic development, has significantly changed the system of relations between society and the media. Traditional media have lost their monopoly on acting as an intermediary between public figures and society in favor of the Internet, which has provided a new type of space and market for social relations. In the new sphere, recipients have gained access to areas that were until recently inaccessible or significantly limited to them. Cyberspace has therefore become a place where people not only receive information provided by others, but also have the opportunity to generate their own content and publish

* *Faculty of Humanities, Koszalin University of Technology, Orcid: 0000-0001-6312-341X*

it. Every Internet user can therefore express their opinion or introduce themselves to a wider audience (Mazurek, 2018: 35). This is due to the social nature of social media, through which functioning within a given network group obliges its users to exchange content. However, in addition to sharing entries, social media is also characterized by the presence of users, which means participation within the structure, "not only by the fact of having an account, but also by connecting the virtual and real spheres" (Mazurek, 2018: 46).

Before the emergence of social media, image creation proceeded differently and concerned the closest environment of individuals. A significant difference that social media has provided in comparison to traditional media is the scale of influence due to greater reach, unlimited accessibility and usability for most users, the speed of dissemination of news and the possibility of updating information on an ongoing basis (even after it has been published) (Gryszel & Zawadzki, 2023: 34).With their expansion and dominance in the everyday lives of recipients, image creation can be done on a global scale. This is proven by numerous situations in which a seemingly ordinary photo or film "conquers" the Internet, and discussions about it are undertaken by thousands or even millions of users around the world. Internet users who want to share their opinions with others and build their own brand currently have a huge area to use in the form of numerous social networking sites and Web 2.0 resources. However, due to the fact that cyberspace is subject to very dynamic changes, its users are constantly faced with new challenges. On the other hand, providing new tools to reach recipients, it is necessary to constantly adapt to the conditions of the network community.

This chapter shows the importance of the Internet and the ability to use modern technologies in the field of creating one's own image and personal brand. The first part of the work defines the concept of image, and then focuses on the personal brand and the key principles of building it in cyberspace. The next part of the work concerns the strategy and stages of creating a personal brand. Finally, the last part of the chapter is an indication of the effectiveness factors of social media used to build an image and personal brand. The method used in the work was desk research and analysis of existing material. The analysis used both scientific articles and textbooks addressing the problem of building a personal image and brand in cyberspace.

Image and Principles of Building a Personal Brand in Cyberspace

The image of a person, organization or company is only seemingly an intuitive category (Łączyński, 2018: 80). This concept can be defined broadly, because it is extensive and vague. It means an image, symbol, pattern, prototype, idea, dream

or delusion (Czopek et al., 2016: 81). Therefore, an image can refer to a photo and other graphic representation of an object or person. It is also people's opinion about a specific thing: a country, institution, person, product (Dziewulski, 2017: 184). In connection with this, an image can be defined as an idea of a state or ideal, an equivalent of something, a real similarity to a natural state, an idea of a thing through the senses, ideas, mental image (Czaplińska, 2015: 9).

The introduction of the concept of image to social sciences is attributed by some researchers to Walter Lippmann, the creator of the concept of stereotype (Kochan, 2017: 15). In his 1921 work "Public Opinion", diagnosing the state of society, Lippmann linked the formation of public opinion with the recipient's internal, simplified ideas about public affairs (Lippmann, 1922: 83–88). This author emphasized that the ideas of reality are fragmented and thus deformed. Thus, the image can be defined as "a set of features that, in the view of the recipient, a given entity possesses" (Lippmann, 1922: 88). In this sense, the image is not something static, but is subject to constant reproduction. It can be the subject of active influence from the outside, aimed at shaping it into a desired form (Łączyński, 2018: 80). As Anthony Davis notes, image "is an intellectual or sensual interpretation of a person or object, conditioned by the personal characteristics of the person in whose mind the image is created (emotions, established attitudes, ideas)" (Davis, 2007: 47–48). In turn, Zbigniew Chmielewski, Dariusz Tworzydło and Hubert Ochmański define image as "an image or reflection of the entity's identity in the mirror of the broadly understood market environment". According to the authors, "it is important not only in the process of creating relationships, but also in crisis and difficult situations" for a given entity. It is also not easy to talk about the possibility of obtaining its unambiguous reception, considering the subjective nature of this phenomenon resulting from the assessments given by the environment. Image can be, among other things, the effect of simplifying the reception of the communication process by the recipients and the stereotypes used in their assessments. It is therefore extremely important that it has a positive character, which can be contributed to by actions that are intended to shape and strengthen our brand. However, for this purpose, many levels, communication channels and numerous methods and means by which our image is created must be taken into account (Chmielewski, 2012: 324).

Although, the concept of a personal brand most often appears in the context of people working in the entertainment industries or politics. In reality, it is an essential element of promoting individuals operating in any industry or field (Modrzejewska, 2016: 11). A personal brand can be defined as "a set of unique personality traits, skills and experiences of an individual, the promotion of which is intended to distinguish [him] from the competition" as well as "to build a

positive image of him among members of a specific target group" (Pawluczyk, 2013). Personal branding is therefore a process in which individuals, in order to "stand out from the crowd", present their own value in the professional or personal sphere, by exposing the competences and resources at their disposal (Żukowski, 2017: 21–22). Thanks to a personal brand, one can present one's own needs, values and personalities, influencing the way a given person acts and reacts in various situations (Potgieter & Doubell, 2020: 112). Building a personal brand is therefore about managing the image and related activities. An inherent element of the image strategy and building a personal brand is therefore self-presentation, referred to as "interpersonal self-creation", which is an important factor driving electronic word-of-mouth marketing related to the brand (Jacobson, 2020: 716). It can be defined as a controlled way in which a person is perceived by his or her environment, as well as a style of influencing others in order to elicit a specific reaction (Łapińska, 2016: 37).

There are several foundations of a strong personal brand. The first is visibility, which allows the personal brand to have an impact on recipients. This is achieved by taking on certain specific roles, standing out, having a personality, and acting consistently. What makes a given brand not only visible but also strong is its authenticity (Chimkowska, 2022: 151). The brand image created must therefore be consistent in order to avoid possible stumbles. Recipients follow and evaluate its every move on the web. Therefore, all shared content should be based on the personality of a given individual, their passions, and above all, their values. Following values has an impact on building a competitive advantage for a person who believes in them (Strawińska, 2017: 369). It also helps to achieve a better perception of a person's value, because a brand that inspires trust and sympathy can more quickly convince its recipients to "buy the offer" and familiarize themselves with the published content. By presenting their own image through various communication channels, an individual can therefore consolidate their value as a specialist in a given field. Proper promotion of a personal brand makes it the "go-to" person and expert for a specific target group (Dubey Dewan, 2020: 29). Its authenticity helps to differentiate it from the competition, leading to numerous opportunities, both in professional and social life, as well as in personal life.

Another foundation of a strong brand is authority. In order to build it, it is important to focus activity around specialization and draw attention to knowledge and experience, i.e. what you are an expert in (Chimkowska, 2022: 151). However, in this case, the behavioral and communication resources of your personal image are of great importance (Dubey Dewan, 2020: 36). Having the skills and abilities in the area of self-presentation in public speaking, body language, etiquette or being polite, you can strengthen not only the value of your brand, but also your

education and professional experience. Therefore, in public speaking, skills such as self-confidence and assertiveness are helpful, which also build trust and sympathy. Personal branding is therefore about creating authority and reputation on the market.

Adequate image and personal brand management is helpful in achieving this. In many cases, they require cooperation with experts from various fields, including public relations, digital marketing agencies or leadership coaches (Dubey Dewan, 2020: 37), as well as various types of self-presentation tactics. The latter include describing oneself in such a way as to make a desired impression on others; expressing attitudes that suggest that a given individual has specific features; public attributions, concerning explaining one's own behavior in a way that is consistent with a specific social image; memory manipulation, meaning real or pretended remembering, but also forgetting for self-presentation purposes; non-verbal behavior, i.e. appropriate facial expression, gestures, positioning, and the way one moves; social contacts, through which relationships with certain people are publicly manifested, and relationships with others are severed; conformism and submission, meaning behaving in a way that is consistent with the social norms or preferences of other people; decorations, props, and lighting, i.e. using elements of the environment for self-presentation purposes (Bogdanowska-Jakubowska, 2012: 295).

Strong brands are also associated with specific values, principles and rules that are not relative. Compliance with them is not only protection against an image crisis, but also a basis for building a stable sense of value. Compliance with moral rules is an important introduction to building a network of relationships with people who can also be trusted. Thanks to this, it is possible to create a safe and stable environment for cooperation and development (Chimkowska, 2022: 152). Without a doubt, an authentic personal brand not only complies with specific values and rules, which affects its consistency, but also communicates them to others (Chimkowska, 2022: 153).

Strategy and Stages of Creating a Personal Brand

There are many strategies for building a personal brand. The one that should be adopted depends on the industry in which the entity operates. However, an important issue in this respect is the universal methods of creating an effective brand, which are based on the key issue, i.e. defining its value, what makes a given entity unique and what distinguishes it from others (Akademia Leona Koźmińskiego, 2023). This is achieved by identifying the strengths, passions and skills that a given brand wants to share with others and which contribute to its

success. Research has shown that building a personal brand requires a long-term and complex process (Gouitcheche, 2018: 21). It is evolutionary, organic and (as Hubert K. Rampersad points out) takes place in four specific phases (Rampersad, 2008: 35–37).

Phase one: defining and formulating your personal ambitions. At this stage, you need to identify yourself and determine who you are, what makes me unique and special, what are my values and my genius, what do I represent, what are my dreams. The following questions can help with this: who am I, what are my interests and passions, what do I do, what is my life story (Stawarz, 2015: 17). The brand has to be prepared in an exciting and convincing way. In addition, it is important to make it and its values visible.

Phase two: defining and formulating your personal brand. Creating an authentic, distinctive, coherent, significant and convincing personal brand is the focal point of the actions taken at this stage. However, self-awareness is essential in its construction. A SWOT analysis of your strengths and weaknesses, as well as opportunities and threats, can be used for this purpose. This analysis allows you to assess yourself through four key perspectives: internal, external, knowledge and science, and financial (Rampersad, 2008: 35). The internal part of the SWOT analysis allows you to assess your current strengths (e.g. education) and weaknesses (e.g. communication skills). Thanks to such identification, it is possible to work on weaknesses and improve them in the future. In turn, the external analysis allows you to examine current market trends, including in terms of employment opportunities, or consider threats such as competition on the labor market (Johnson, 2017: 22).

After identifying our personal valuable difference, a strategic projection onto the target group takes place (Gouitcheche, 2018: 21). Thanks to this, it will be possible to determine the leading and most powerful attribute of the entity, its key features and the offer directed to the recipients. It is therefore necessary to define your own target group and its most important needs. Identifying the target market, which may be, for example, a potential employer, will allow you to strengthen the brand's message and emphasize the skills and knowledge of its creator. Once this is done, it is possible to move on to the next stage, within which the personal story of the brand will be defined, which is de facto the essence of what you want to say about it to evoke a positive emotional response. Such a personal brand story gives individuals the opportunity to stand out from the crowd. To this end, it is necessary to personally identify what you do and why it is so unique that people will be interested in it. An example of a brand story might look like this: "I am an entrepreneurial technology marketer with a passion for building teams of brand advocates by cultivating relationships with customers and users" (Johnson, 2017: 22).

Phase three: preparing your personal and balanced scorecard, or personal brand statement. In this phase, it is important to develop an integrated and well-balanced action plan based on your personal brand and ambitions. This will allow you to achieve your planned goals, but also eliminate all negative elements. Your personal brand and potential tasks translate into manageable measurements and personal goals, milestones, and corrective actions in a balanced, holistic way (Rampersad, 2008: 36). Preparing a plan is essential for improving your brand and developing your own skills. It can be used to develop future improvement actions, track progress, capture key brand information, define new career paths, and build networks and report on achievements (Rampersad, 2008: 36).

Phase four: implementing and improving the personal brand. A personal brand must be expressed through passion and love. The person who builds it should therefore be committed to change and constantly improve the perception of their own value on the market (Rampersad, 2008: 36). A personal brand is in fact the image and reputation of a person who is recognizable in their professional environment. Therefore, it is important to build credibility and the status of an expert in their field and to disseminate information about themselves through various media channels. The brand therefore requires constant updates that reflect new challenges and learning from the actions taken and personal development. This ensures the strengthening, maintenance, protection and development of the brand (Rampersad, 2008: 36).

An important issue for creating an effective brand is, above all, the appropriate selection of communication channels through which we will present it. Today, supporting promotional activities through social media is of great importance. An essential element of promoting any brand is therefore an effectively planned image on the Internet. Nevertheless, using all available channels can lead to a loss of credibility and a lack of intended effects. Therefore, the best way is to choose platforms that are potentially the area best suited to our activity, and thus a place where we will find our recipients. Appropriate and dedicated targeting turns social media platforms into an arena of personal branding for people who want to create the desired awareness (Joseph, 2018). Intensification of activity in channels adapted to the brand's activity and the recipients interested in it undoubtedly helps to achieve the intended goals developed during its creation. However, in order to create the desired brand image in social media, not only the creator's intention is important, but also taking communication actions and examining how the brand is received and what results our activity on the network achieves (Jasiulewicz & Kozyra, 2017: 223).

This is why social media should not be viewed solely as platforms for publishing content. Their essential feature is the ability to establish contacts and

communicate. They are also a source of quick problem-solving. When having a public profile on social media, you should be open to all questions, doubts and problems of recipients (Sopiak, 2023). Questions appearing under a photo or post, but also in private correspondence, should be met with a response. Users of social platforms treat them as a channel of quick communication, which is why they expect an almost immediate response. Creating value in social media cannot therefore be described as a one-way (Karaduman, 2013: 472). Personal interactions build brand trust (Rangarajan, 2017: 4) and in order to gain awareness and loyalty of recipients, you should cooperate with them and show your interest.

Social Media Effectiveness Factors in Building a Positive Image and Personal Brand

As Denis McQuail notes, there are seven main features, or dimensions, which have a direct impact on the characteristics of contemporary users and on certain marketing concepts (Grębosz 2016: 34) also in terms of building one's own image and personal brand on the web. The first of these is interactivity, which is the rate of response from users to the sender's message. It refers to the ability to send a message that is simultaneously answered. Another dimension is social presence, which allows for a sense of personal relationship with other users of a given platform. Through a sense of accessibility, communication with recipients becomes more authentic and can be significantly appreciated by them (Chimkowska, 2023).

Richness is also an important factor that has a direct impact on user characteristics and, consequently, on marketing concepts. This dimension concerns enabling communication through various forms of feedback, verbal, visual, and auditory (Grębosz 2016: 34–35). The more feedback options a medium has, the richer it becomes. In this respect, instant messaging is considered the best, as it allows for face-to-face conversation. The "richness level" is, for example, low in the case of collective projects and blogs, because they are largely text-based and allow only limited exchange of information. On the other hand, content communities and social networking sites receive an average rating in this respect. In their case, users can share photos, videos, and other types of materials in addition to text messages. In terms of social presence and richness, virtual games and social worlds are rated the best. Thanks to them, it is possible to open up various dimensions of face-to-face interaction. Nevertheless, the best opportunities for self-presentation are provided by social networking sites (Gryszel & Zawadzki, 2023: 35).

The fourth dimension indicated by McQuail is playfulness, which means that for users, social media do not fulfill a purely utilitarian or informational function.

In their case, the fact that they provide pleasure and entertainment is of great importance. Another feature is privacy. Communication in new media focuses more on the subjective than the objective. Using media is not purely instrumental, but rather refers more to emotions and expressing one's own feelings. Finally, personalization, which concerns the both the message and the way of use (McQuail, 2007: 149–156). In this case, it is about the degree to which the message of a given medium is tailored to a specific user, e.g. by using data that one has about the recipient (Gręboszz 2016: 34–35).

Social media has become a new arena for "identity creation, performance, and management" (Jacobson, 2020: 716). Using social media involves combining information and presenting it in a system through which identity is created and "consumed" by online recipients. Communication through electronic devices allows individuals to present a more positive version of themselves than is possible in interpersonal communication (Jacobson, 2020: 716). Each social media user has the opportunity to become a content producer and present it through interactive communication based on a pyramid of relationships (Karaduman, 2013: 467). In the online context, personal brand identity is based on self-presentation. This is because brands are created in computer-mediated environments, using social media profiles, websites, and blogs (Labrecque, 2011: 44).

An important feature and factor in the effectiveness of social media in building a brand image is the ability to increase social capital, which refers to the skillful use of resources and engaging in mutually beneficial social cooperation through social networks. The concept associated with brand management in this area is therefore the "idea". It refers to the fact that a personal brand is a process that describes standing out from the crowd of entities by presenting a unique value proposition based on personal abilities and a specific profession (Nowakowska, 2019: 26). The image built in this way is then used with a coherent message in order to achieve its goal. As research shows, personal branding offers individuals a chance to increase their social capital and a way to flexibly adapt to changing labor markets (Johnson, 2017: 22). However, in order to create a positive image of a personal brand, cooperation with others, exchange of experiences and a desire to deepen one's knowledge are necessary. Therefore, an important factor in achieving this goal and thus promoting the brand is participation in conferences and industry events, thanks to which it is easier to build a network of contacts with other representatives of the field of interest to us. Image promotion in face-to-face contacts is therefore intended to be, in a sense, a complement to the brand shaped through electronic media (Trzeciak, 2015: 29).

Social media are also considered to be potentially the most powerful tool in business practice, which is why they are used intensively to implement strategies at

lower costs (Karaduman, 2013: 467). However, promotion on the Internet should not be a goal in itself, but should be solely a means of creating one's own personal brand. The image on the Internet must therefore be consistent with our brand and, in a sense, extend the range of our influence in relation to traditional methods of direct contact with business partners, clients or co-workers.

Conclusion

The Internet, and especially social media, have become one of the greatest sources of changes that have occurred in communication in recent years. The popularity of social networking sites has also increased significantly, which is associated with the trend of user activation. Social media not only allow for passive reception of content, but have also enabled access to active shaping of their resources. Also in the case of creating an image and building a personal brand, media play a key role today. Social platforms provide the opportunity to reach a wide audience, have direct contact with them, and create a coherent and more positive image of a personal brand than could be the case in the real world. Although until recently having a personal brand was the domain of celebrities only, today everyone has their own brand, although not all people are aware of it. This is why, in the era of digitalization and constant change, it is necessary not only to skillfully use the tools that are social media, but also to constantly update the strategy for creating one's own image and personal brand and improve it.

References

Akademia Leona Koźmińskiego. 2023. *Jak budować markę osobistą? Poznaj sprawdzone strategie personal brandingu* [How to build a personal brand? Learn proven personal branding strategies]. Accesed August 31, 2024. https://www.kozminski.edu.pl/pl/review/jak-budowac-marke-osobista-poznaj-sprawdzone-strategie-personal-brandingu.

Bogdanowska-Jakubowska Ewa. 2012. „Strategie tworzenia wizerunku własnego w dyskursie politycznym" [Strategies for creating one's own image in political discourse]. In: *Transdyscyplinarność badań nad komunikacją medialną. T. 1, Stan wiedzy i postulaty badawcze* [Transdisciplinarity of media communication research. Vol. 1, State of knowledge and research postulates], edited by M. Kita, M. Ślawska (red.), Katowice : Wydawnictwo Uniwersytetu Śląskiego.

Chimkowska Angelika. 2022. *Autentyczny personal breanding – czyli silna marka osobista w praktyce* [Authentic personal branding – a strong personal brand in practice]. Warsaw: MTbiznes.

Chimkowska Angelika. 2023. *Marka Osobista CEO Branding dobre praktyki #SMwP S03E11* [Personal Brand CEO Branding good practices #SMwP S03E11]. Accesed August 31, 2024. https://silnamarka.com/marka-osobista-ceo-dobre-praktyki/.

Chmielewski Zbigniew et al. 2012. „Budowanie wizerunku w sieci - możliwości i zagrożenia" [Building an image on the web - opportunities and threats]. *Marketing Instytucji Naukowych i Badawczych*, vol. 4, no. 3, pp. 321–329.

Czaplińska Paulina. 2015. „Strategia budowania wizerunku osób znanych" [Strategy for building the image of famous people]. In: *Perswazyjne wykorzystanie wizerunku osób znanych* [Persuasive use of famous people's images], edited by Adam Grzegorczyk. Warsaw: Wyższa Szkoła Promocji, Mediów i Show Businessu.

Czopek Miłosz et al. 2016. „Rola mediów w kreowaniu wizerunku" [The role of media in creating an image]. *Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych*, vol. 9, pp. 79–94.

Davis Anthony. 2007. *Public relations*. Warsaw: Polskie Wydawnictwo Ekonomiczne.

Dubey Dewan Sonia. 2020. "The Role of Personal Image in Personal Branding". *Cuadernos Del Centro De Estudios De Diseño Y Comunicación*, no. 118, pp. 29–38.

Dziwulski Jacek. 2017. „Kreowanie wizerunku organizacji na przykładzie Spółdzielni Pszczelarskiej „Apis" w Lublinie" [The Creation of the Image of an Organization on the Example of "Apis" Apiculture Cooperative in Lublin]. *Marketing i Zarządzanie*, vol. 47, pp. 183–195.

Gouitcheche Emmanuel. 2018. "Brand identity and brand image: personal branding in the music industry". *Lietuvos aukštųjų mokyklų vadybos ir ekonomikos jaunųjų mokslininkų Konferencijų darbai*, no. 21, pp. 17–26.

Gręboszc Magdalena et al. 2016. *Social Media Marketing*. Łódź; Wydawnictwo Politechniki Łódzkiej.

Gryszel Piotr & Piotr Zawadzki. 2023. „Cele i formy aktywności marketingowej polskich miast w mediach społecznościowych" [Goals and forms of marketing activity of Polish cities in social media]. *Studia Periegetica*, vol. 2, no. 42, pp. 31–49.

Jacobson Jenna. 2020. "You are a brand: social media managers' personal branding and "the future audience"". *Journal of Product & Brand Management*, vol. 29, no. 6, pp. 715–727.

Jasiulewicz Anna & Alicja Kozyra. 2017. „Wykorzystanie mediów społecznościowych w kreacji wizerunku marki na przykładzie linii lotniczych"

[Using social media in creating a brand image on the example of airlines]. *Handel Wewnętrzny*, vol. 5, no. 370, pp. 222–230.

Johnson Katryna M. 2017. "The Importance of Personal Branding in Social Media: Educating Students to Create and Manage their Personal Brand". *International Journal of Education and Social Science*, vol. 4, no. 1, pp. 21–27.

Joseph Jerome. 2018. *10 Key Trends for Personal Brands*. Australia: Global Brand Academy. https://theglobalbrandacademy.com/wp-content/uploads/2018/10/10-Key-Personal-Brand-Trends-Whitepaper-2.pdf.

Karaduman İlkay. 2013. "The effect of social media on personal branding efforts of top level executives". *Procedia - Social and Behavioral Sciences*, vol. 99, pp. 465–473.

Kochan Marek. 2017. „Język a wizerunek polityków" [Language and the image of politicians]. *Studia Politiologiczne*, vol. 45, pp. 13–45.

Labrecque Lauren I. et al. 2011. "Online Personal Branding: Processes, Challenges, and Implications". *Journal of Interactive Marketing*, vol. 25, pp. 37–50.

Lippmann Walter. 1922. *Public opinion*. New York: Harcourt Brace and Company.

Łapińska Karolina. 2016. „Postrzeganie celebrytów dawniej i dziś. Autokreacja wizerunkowa kontra wizerunek medialny" [Perception of celebrities in the past and today. Self-image creation versus media image]. In: *Dyskurs autopromocyjny dawniej i dziś* [Perception of celebrities in the past and today. Self-image creation versus media image], t.2, edited by Aleksandra Kalisz, Ewelina Tyc. Katowice: Wydawnictwo Uniwersytetu Śląskiego, pp. 31–41.

Łączyński Marcin. 2018. „Wizerunek" [Image]. In: Metody badania wizrununku w mediach [Methods of researching image in the media], edited by Tomasz Gackowski, Marcin Łączyński, Warsaw: CeDeWu, pp. 79–104.

Mazurek Kamil. 2018. *Facebook. Od portalu społecznościowego do narzędzia polityki* [Facebook: From Social Network to Policy Tool]. Lubiln: Wydawnictwo Uniwersytetu Marii Curie Skłodowskiej.

McQuail Denis. 2007. Teoria komunikowania masowego [Mass Communication Theory]. Warsaw: Wydawnictwo Naukowe PWN.

Modrzejewska Ilona. 2016. „Budowanie marki osobistej przez pracownika" [Building a personal brand by an employee]. In: *Zarządzanie w XXI wieku – koncepcje organizacji przyszłości*, edited by Aleksandry Szejniuk i Małgorzaty Kaniewskiej, Józefów: WSGE.

Nowakowska Gabriela. 2019. „Budowanie marki osobistej na przykładzie marki Macieja Bodnara" [Building a personal brand on the example of Maciej Bodnar's brand]. *Marketing i Rynek/ Journal of Marketing and Market Studies*, no. 8, pp. 25–37.

Pawluczyk Piotr. 2023. *Marka osobista – czym jest, rodzaje, przykłady* [Personal brand – what is it, types, examples]. Accesed August 31, 2024. https://cyrek-digital.com/pl/baza-wiedzy/marka-osobista/.

Potgieter Adele & Marianne Doubell. 2020. "The influence of employer branding and employees' personal branding on corporate branding and corporate reputation". *African Journal of Business and Economic Research (AJBER)*, vol. 15, no. 2, pp. 109–135.

Rampersad Hubert K. 2008. "A new blueprint for powerful and authentic personal branding". *Performance Improvement*, vol. 47, no. 6, pp. 34–37.

Rangarajan Deva et al. 2017. "Strategic personal branding–And how it pays off". *Business Horizons*, vol. 60, no. 5, pp. 657–666.

Sopiak Sylwia. 2023. *Wizerunek w Social Media – 5 dobrych praktyk* [Image in Social Media – 5 good practices]. Accesed August 31, 2024. https://harbingers.io/blog/wizerunek-w-social-media-5-dobrych-praktyk.

Stawarz Barbara. 2015. *Content Marketing po polsku. Jak przyciągnąć klientów* [Content Marketing in Polish. How to Attract Customers]. Warsaw: PWN.

Strawińska Anetta Bogusława. 2017. „Historia i definicja terminu personal branding. Zarys problematyki" [History and definition of the term personal branding. Outline of the problem]. In: *Socjolekt - idiolekt - idiostyl : historia i współczesność* [Sociolect - idiolect - idiostyle: history and present day], edited by Urszula Sokólska. Białystok: Wydawnictwo Prymat.

Trzeciak Sergiusz 2015. *Wizerunek publiczny w internecie. Kim jesteś w sieci* [Public Image on the Internet. Who You Are Online], Gliwice: Wydawnictwo Helion.

Żukowski Marcin. 2017. *Ty w social mediach. Podręcznik budowania marki osobistej dla każdego* [You in Social Media: A Guide to Building a Personal Brand for Everyone]. Gliwice: Helion.

Oleksii Novikov, Iryna Stopochkina, Kostiantyn Ilin, Mykola Ovcharuk, Mykola Ilin, Andrii Voitsekhovskiy, Lesia Alekseichuk*

Ensuring the Resilience of Critical Infrastructure Employees Against Social Engineering Attacks

Abstract: Based on the mathematical and algorithmic framework developed by the authors, a software package has been created. It performs functions to increase the resilience of personnel of critical infrastructure facilities of the regime type to social engineering attacks that occur through the social, socio-technical, and socio-physical vectors. The software package performs diagnostic, training, and decision support functions. The decision support module is based on the modification of the SEADM (Social engineering attack detection model) algorithm proposed in this paper, which is characterized by a focus on the specifics of critical infrastructure facilities of the regime type and decision-making in a short time frame. The diagnostic and training module is based on a questionnaire previously developed by the authors, with cases and their analysis of popular situations targeting critical infrastructure facilities in Ukraine.

The paper establishes the correspondence between the threat techniques according to the MITRE classification and the types of social engineering impacts that can be used by an attacker. The proposed software package allows for flexible modification to the needs of the enterprise due to the possibility of making independent changes to the questionnaire, presented in a structured format, according to the relevant techniques and impacts of social engineering.

Keywords: human factor, social engineering, critical infrastructure, resilience

1. Introduction

The number of cybersecurity incidents that occur due to human factor exploitation continues to grow. Massive attacks on critical infrastructure facilities actively exploit the vulnerabilities of personnel, as this is an easier way to achieve the goal than attempts to hack cybersecurity systems that are constantly monitored and improved. The human factor remains a weak link in the security system of any enterprise, and this is especially true for critical infrastructure facilities that require increased attention to cybersecurity (Krombholtz et al., 2013).

Paper (Shevchenko, Stopochkina and Babenko, 2022) analyzes the dynamics of cyberattacks that use social engineering since January 2022 in Ukraine and shows a lack of solutions to improve the existing situation.

* *National Technical University of Ukraine "Igor Sikorsky KPI"*

Papers (Zetter, 2014; Gallagher, 2016; Lee et al., 2016; Liptak, 2016; Sanger, Krauss and Perlroth 2021; Tidy, 2021) showed the possibilities of using the human factor and further cyberattacks that developed due to the successful conduct of a social engineering attack. Namely, in (Zetter, 2016) the features of an attack on a nuclear facility (Stuxnet) are discussed, analytical paper (Lee, 2016) analyzes an example of an attack on the energy system (BlackEnergy attack on Prykarpattia regional power distribution companies), articles (Sanger, 2021; Tidy, 2021) show the stages of a cyberattack on the oil industry, and papers (Liptak, 2016; Gallagher, 2016) are devoted to attacks on transport facilities.

The success of a social engineering attack in all of the above cases is a guarantee of obtaining the necessary information or privileges by the attacker, which makes further unauthorized interference possible. There are many trainings and tools available to train employees' vigilance in countering social engineering attacks.

However, the scale of the social engineering problem shows that existing tools and approaches are not sufficient, which makes the development of the software package presented in this paper relevant.

Active work on the means of preventing social engineering attacks has led to the emergence of trainings in this area and penetration testing solutions. The tools listed below are based on algorithmic content that uses research on actual cyberattacks using the human factor (Mataracioglu and Ozkan, 2011).

Among the existing tools, it is worth noting (KnowBe4, 2024), which offers training to identify the level of cybersecurity awareness of users, simulate phishing attacks, and provide cases for processing. The tools (Barracuda, 2019) are notable for their complexity of use and are aimed at training users. The training (Cofense, 2024) works out situations of bypassing email filters that can be used by an attacker. The disadvantage of this solution is a weak focus on the needs of a critical infrastructure facility, with the emphasis being placed only on mail vector attacks, although there is a wider variety of them. The test offered on the resource (DataArt, 2019) provides a means of penetration testing through social engineering attacks by emulating real situations for enterprise users. These types of tools use examples of known attacks and train users to recognize them. However, at the same time, they do not analyze why a person reacts positively to the social engineer's suggestions. That is, the only experience the user gains is knowledge of how to act in a certain list of situations, without a clear understanding of the root reason causes associated with the weaknesses of human nature. Similar methods and ideas for improving employee resilience to social engineering attacks are discussed in (Arachchilagea and Love, 2014).

A common feature of these and many other works and tools is that they are focused on training and/or testing users based on specific cases of social

engineering attacks that are quickly becoming outdated. At the same time, the reason for the success of such attacks, which is the user's vulnerability, not always related to employee ignorance, remains unaddressed. This paper proposes a diagnostic module that combines the principles of training tools. The module is based on a list of social and psychological characteristics that make a person vulnerable to a number of social engineering attacks.

The study of human characteristics that make a person vulnerable to social engineering attacks was carried out in (Mitnik and Simon, 2003; Bhakta and Harris, 2015; Mouton et al., 2014). The paper (Mouton et al., 2014) contains the idea of building a taxonomy of social engineering attacks and their dependence on exploited factors. The paper (Shevchenko, Stopochkina and Babenko, 2022) contains examples of common social engineering attacks during Russia's full-scale invasion of Ukraine, which helps to understand the human weaknesses used in this time.

Some of the human weaknesses can be eliminated in advance, regardless of the type of attacks that may be used. For example, you should pay attention to risk-taking, excessive trust, inability to say "no", and fear of management. The questionnaire is designed in such a way that the questions reveal these and other vulnerabilities, as well as teach the respondent how to act in the situation specified in the question.

The survey consists of three parts: the first part is aimed at identifying vulnerabilities in the context of attacks that are inherent in the social environment (without the involvement of any additional technical means), the second part identifies user vulnerabilities and shortcomings in the security policy of a critical infrastructure enterprise to attacks in the socio-technical environment (i.e., those carried out with the involvement of e-mail, messengers, specialized programs used by a social engineer). The third type of survey is aimed at identifying organizational shortcomings in the enterprise's work and vulnerability to attacks through the socio-physical environment (for example, using the peculiarities of the access control mode, and physical media).

A large number of cyberattacks can be carried out using social engineering. This paper draws a connection between the MITRE attack techniques for critical infrastructure (MITRE, no date) and social engineering-based impacts. To achieve the goal, attackers can use the vulnerabilities of personnel, some of whom, under certain conditions, may become conscious or unconscious accomplices of the social engineer. As a rule, these are employees who demonstrate disloyalty to the company, self-interest, aggressiveness, and other signs that can serve as indicators of a potentially dangerous situation. A list of such signs, detailed description of the relevant profiles, and a methodology for their detection are proposed in the authors' previous study (Ilin and Stopochkina, 2024). To identify such features, it is proposed to use the approaches of sociological surveys. In particular, there are survey tools and appropriate theoretical background are proposed. In particular,

papers (Anderson and Bushman, 2002; Dupre and Barling, 2006; Kersten and Greitemeyer, 2024) are devoted to identifying the nature and level of aggressiveness, technical review (Knapp, Heggestad and Young, 2004) consider the issues of motivation testing, paper (Bustamante, Davis and Marques, 2014) considers the issues of testing diligence and industriousness, resource (TestPartnership, 2023) demonstrates an example of comprehensive testing of an employee in several areas, resource and article (PE Konsult LTD, 2016) provide a background for employee responsibility test, and the testing tool (Parvez, 2024) is aimed at identifying the level of self-interest. The diagnostic module proposed in this paper is based on Boolean functions to identify a set of features (profiles) that determine the user's increased vulnerability to social engineer proposals. The profiles can also be used at the stage of building a formalized model of an internal offender. The peculiarities of the surveys conducted for representatives of the staff of critical infrastructure facilities in Ukraine are discussed in (Ilin and Stopochkina, 2024).

An important aspect of increasing the resilience of critical infrastructure employees to social engineering attacks is to provide decision support for suspicious requests. This is primarily relevant for those employees who are in contact with outsiders and provide certain rights or information in response to their requests. These can be employees working with customers, suppliers, and support staff. The decision support module included in the proposed package is based on a modification of the SEADM algorithm (Bezuidenhout, Mouton and Venter, 2010), which is proposed in this paper. When developing the decision support module, it was decided to use a clear algorithmic structure, instead of applying machine learning methods, to avoid false positive or false negative answers and to ensure transparency of recommendations. The algorithm, unlike the existing one, takes into account the short decision-making time, the specifics of requests that may be submitted at a critical infrastructure facility, and the need to share responsibility with security services and other authorized persons.

2. Examples of cyberattacks that use human factor

Here are examples of attacks on critical infrastructure facilities that use social engineering (Ghafir et al. 2018).

Stuxnet, attack on nuclear facility in Natanz, Iran. The attack began with pretexting and open-source reconnaissance, which allowed the creation of a legend for the introduction of an insider employee into the company.

The second stage of the attack involved the use of social engineering with the use of infected media (the media was placed in places where it could be picked up by employees of the facility).

Employees who mistakenly or unknowingly used the planted media connected it to the company's internal network. As a result, the Stuxnet malware spread and gained control over programmable logic controllers and the process monitoring system.

The consequence of this attack was a change in the speed of rotation of centrifuges at the nuclear facility, which led to damage without arousing suspicion among system operators. *BlackEnergy, attack on energy company of Ukraine.*

The attack began with phishing emails containing malicious attachments in disguise to gain access to the company's network.

The next step was the activation of the malware by employees who opened the attachments. The malware gained access rights to the internal information system, and BlackEnergy and KillDisk malware were introduced, gaining control over the supervisory control and data acquisition system.

The consequences of such an attack were power outages in the western regions of Ukraine.

Attack on San Francisco subway.

The attack began with the exploitation of human factor vulnerabilities by conducting a phishing attack through emails with malicious links disguised as messages from official partners or internal departments.

Clicking on the malicious links resulted in the installation of ransomware on the internal system. At the next stage, the malware encrypted data and blocked access to the fare payment systems.

The attack resulted in financial losses, data loss, and disruption of transportation.

Attack on gas pipeline company, USA.

First, the attackers carried out a phishing attack on employees, which allowed them to gain access to the internal system and exploit existing vulnerabilities. Next, they installed ransomware on the servers that controlled the operation of the gas pipeline, which led to data inaccessibility. The consequences were interruptions in fuel supply to the United States east coast, and restrictions or termination of oil product supplies.

From the examples, we can see that social engineering attacks are usually the first step to a successful cyberattack, and open an entry point to the internal systems of a protected object by exploiting human vulnerabilities. Thus, we can observe here the chain: human factor – cyberattack – physical disruption of the system. Next, we take into account human vulnerabilities, so the chain takes the following form: human vulnerable features – social engineering attack – cyberattack – physical disruption of the system.

3. The principles of software package functioning

3.1 Diagnostic module. Sets of employee vulnerabilities

To diagnose personnel vulnerabilities to social engineering attacks, a questionnaire should be designed that contains questions that can identify potential weaknesses of the person that reveal themselves in certain situations. These can be personal traits or universal qualities that can be inherent in anyone in certain conditions.

Let's highlight the characteristics of the employee that may signal a susceptibility to the effects of social engineering. The corresponding approach was proposed in (Krombholz, 2013; Mouton, 2014).

Let's highlight the personal factors, which can be triggers for various social engineering attacks:

- fearfulness, timidity T1;
- inability to refuse T2;
- inability to limit oneself when obtaining something (greed, including for work, gambling, etc.) T3;
- carelessness T4;
- ignorance T5;
- tendency to laziness or procrastination T6;
- indifference T7;
- unpunctuality T8.

Let us explain the terms used.

The tendency to fear implies fear of management staff, certain uncomfortable circumstances that may provoke disapproval of the victim's actions by the community, and other fears. A social engineer can fraudulently pass off his illegitimate requests as orders from managers, exert veiled pressure on the victim, indicating the bad consequences that will occur if his request is not fulfilled.

The inability to refuse is a handy quality for a social engineer who tries to frame a request in such a way that the victim agrees to fulfill it, even contrary to security policy.

The inability to limit oneself makes a person vulnerable to offers of useful resources and participation in activities organized by a social engineer according to the victim's preferences.

Carelessness and ignorance are factors that imply an insufficiently high level of employee qualification in countering cyberattacks, which use the human factor. These shortcomings should be eliminated through special training and professional development.

A tendency to laziness and procrastination can be used by a social engineer to offer "easy" solutions to bypass security policies.

Indifference is exploited as a factor that ensures impunity for the actions of a social engineer and minimal interference in his operations by indifferent personnel.

Non-punctuality is associated with inaccurate compliance with various instructions and guidelines of the security policy, which can be used in attacks on the information system.

The proposed module is based on the principle of matching the respondent to a profile determined by a set of traits.

Some of the profiles signal potential danger and characterize people who are vulnerable to social engineering attacks.

Let's list such profiles:

1. {T1 and T2 and T7} is a profile that corresponds to a soft person who is easy to manipulate. Even if she notices a violation, it will be easier to keep quiet about it.
2. {T3 and T5 and T6} is a profile that corresponds to an active person who seeks to obtain various benefits. However, the person is prone to laziness and is not interested in the possible consequences of decisions. This allows a social engineer to offer options for easy profit and cybersecurity violations.
3. {T4 and T7 and T8} is a profile that corresponds to a careless person who is not punctual and attentive. Ignorance increases vulnerability to attacks that rely on impulsive, rash decisions.
4. {T3 and T4 and T7} is a profile that corresponds to a person who is risk-averse and rather indifferent to the negative consequences of actions.

The presence of these qualities in a personality profile should be determined by means of a questionnaire. The questionnaire offers questions that correspond to the factors listed above or a combination of them. A factor is considered to be present, and the corresponding Boolean variable is true when the survey shows that the numerical score of this factor exceeds the group average.

From the point of view of analyzing the qualities of a critical infrastructure employee who has access to important information or system functions, the most dangerous personal factors are: carelessness, lack of professional and related knowledge, indifference, and unpunctuality. These signs may indicate a disrespectful attitude to work or an unwillingness to realize its importance, which is unacceptable for employees of industrial critical infrastructure facilities. Correction of these factors does not require the involvement of a psychologist but is achieved by drawing attention to their presence, as well as through training to improve skills and motivational measures that promote the development of the necessary qualities.

In addition to social and socio-physical characteristics, it is also necessary to consider socio-technical characteristics, which are not entirely dependent on personal and social factors but are largely determined by the critical infrastructure

facility's security policy. The questions in the socio-technical questionnaire are aimed at assessing the employee's understanding of the company's security policy, the availability of clear instructions and restrictions on dangerous actions, and verifying the implementation of appropriate technical and organizational measures. After all, even the most cautious and knowledgeable employee can be vulnerable to cyberattacks carried out through social engineering if the company does not provide appropriate technical means to prevent harmful effects.

The questions in the questionnaire can be scored on a different scale. For example, some questions may contain multiple-choice (checkbox) answers, while others may contain single-choice (radio button) answers. When evaluating, it is necessary to normalize the results by bringing them to a common scale.

The weights of questions can be calculated using the Saaty pairwise comparison method if we have a large number of survey types and it is difficult to prioritize each type at once.

The availability of an overall score can allow employees to be ranked according to their potential resistance to social engineering attacks.

It is also possible to calculate the person's score in the areas of {T4, T5, T7, T8}, which are critical in terms of working at a sensitive facility and access to sensitive data.

It is also interesting to analyze the scores in the areas of personal factors {T1…T7}.

Similarly, the questions in the questionnaire can be grouped by factors to which any person is sensitive in certain situations:

- Strong influence (F1),
- Reciprocity (F2),
- Overload (F3),
- Lack of something (F4),
- Deceptive relationships (F5),
- Urgency (F6),
- Social approval (F7).

Let us explain the terms used.

- Strong influence means telling the victim shocking news, introducing force majeure situations that threaten safety, and other actions that can put the victim in a state of severe nervous tension.
- Reciprocity means actions that imply a reciprocal response and put the victim in a state of obligation.
- Overload - providing the victim with a large amount of confusing information that is difficult to understand in a short period of time.
- Lack of something means a situation that implies the victim's need for some action or resources (for example, lack of communication, need for software that is difficult for the victim to acquire in a normal way, etc.)

- Deceptive relationship appears when a social engineer makes the victim believe that they have a friendly relationship (friendship, partnership, etc.) with the attacker, which obliges the victim to respond accordingly.
- Urgency takes place when social engineer requests something that must be fulfilled immediately, otherwise there will be a threat of an unpleasant situation.
- Social approval is exploited by putting the victim in a state where fulfilling a request that is beneficial to the social engineer will give the victim a sense of community approval or self-worth (e.g., fulfillment requests for charitable donations).

We can calculate the total score for one or more factors. Each social engineering attack has its own pattern that uses a particular factor. For example, vishing often exploits factors F1, F3, and F6. Pretexting via messenger uses factors F4 and F5. Similarly, different types of phishing attacks can use F7, F2, or other factors. The higher the score an employee gets on this type of question, the more resistant they are to the exploitation of this type of factor.

The questionnaire also groups questions by attack vector environments. The following are highlighted: physical environment, e-mail, messenger, web resources, social networks, telephone, and personal communication.

The results of the survey are summarized in the form of a profile built in the form of a "wind rose", with personal and general vulnerabilities being highlighted as areas of focus (Fig. 7).

3.2 Module in training mode and diagnostic results

A questionnaire was developed for the testing of employees of the critical infrastructure facility. Questions, answer options, and points are presented in a structured form in JSON format. The parser reads the questions and presents them and the answer options in the user interface. Each question is followed by an analysis of the situation proposed in the question, which argues for the correct answer. Thus, not only person vulnerabilities are diagnosed, but also simultaneous training is provided.

A number of questions are designed in such a way as to reveal weak links in the security policy of a critical infrastructure enterprise. Emphasis is placed on regulatory measures, the presence of clear orders and instructions on cyber security, instructions for actions in force majeure circumstances, the composition and procedure for using software and hardware at the workplace.

The training mode of the diagnostics module (Fig. 1–3) is used to achieve the training effect. After passing each question, to which the person gave his answer, he is provided with an analysis of the situation, with an explanation of the correct course of action. Explanations for each question are included in the questionnaire

in JSON format. If possible, it is desirable for each situation to be commented on by a trainer who would draw the trainee's attention to key points for better assimilation of information. An example of a question and explanation is given in table 1. The view of the question for the employee is presented in Fig. 1.

The survey also makes it possible to identify certain shortcomings of an organizational and technical nature that are inherent in the object of critical infrastructure on which the survey is carried out: in particular, the absence of prohibitions on the installation of third-party software, the use of third-party media, the absence of clear regime and transit rules, unprotected document flow, unprotected business communication, etc.

Table 1: Structure of the questionnaire and examples of questions

Environment, psychological factor, personal factor	**Question**	**Action options (single / multiple choice) are evaluated by points**	**Explanation in the application report**
Socio-technical environment, (Email). Negligence.	On behalf of an employee entrusted to you, a letter was received, with recommendations to pay attention to the existing results of awards for the best employees selected by the results of the year. The email contains a link to an external resource.	1. Open the link because you have an antivirus installed and your browser has its own sandbox. 2. Check the link for maliciousness in a specialized online resource. 3. You are not interested in surveys, you will definitely not become the best employee of the year 4. You call your employee to find out what kind of resource it is. If the information is confirmed, open the link. 5. All information at my company comes through the electronic document management system with an electronic signature.	There is malware. which may be located at the link, which is not recognized by the antivirus and breaks the browser sandbox. Therefore, it is better to check all links for harmfulness additionally. Orderly electronic document flow through a secure system of document flow nullifies the attempts of a social engineer to disguise himself as an employee, or to forward illegitimate attachments - this is the best option.

Environment, psychological factor, personal factor	**Question**	**Action options (single / multiple choice) are evaluated by points**	**Explanation in the application report**
Inability to refuse, reciprocity Social environment	A friend introduces you to a company where everyone tells witty life stories about account attributes, what phrases and combinations they use to log into the account. "Now it's your turn to tell," says your friend.	1. You say that nothing interesting happened in your life related to passwords. You usually use random combinations of numbers and letters that you keep in your notebook. Everyone looks at you like a bore. 2. You tell some interesting details without giving away the details. For example, you sometimes use a phrase from your favorite song. 3. You say that you save passwords in a password manager. And you don't know anything by heart, because you usually log in from the same device using O-Auth2. 4. You refuse to tell. Those around you insist, but you are adamant. 5. You say you have created a strong password, but it is the same for all accounts.	It can be dangerous to share any details about your password. If the password is stored in a password manager, an attacker can try to gain unauthorized access by taking over your device or asking to use it for a period of time. Some password managers may also be vulnerable to cyber attacks. In no case should you make one password for all services - not all of them are equally reliable, and after learning about this, an attacker can start trying to attack more vulnerable ones in order to find out the password by hacking or other methods.

(*Continued*)

Table 1: (Continued)

Environment, psychological factor, personal factor	**Question**	**Action options (single / multiple choice) are evaluated by points**	**Explanation in the application report**
Socio-physical environment, lack (in this case, the need for media), interest	You find someone's flash drive in the corridor	1. You hand over the find to the information security department. 2. Study the contents of the flash drive independently at the workplace. 3. You study the contents of the flash drive at home by connecting it to an isolated workplace. 4. You format the flash drive and put it off until better times if you suddenly need it.	Flash media can be not only a means of spreading software viruses, which can be destroyed by media formatting but also hardware virus embedding, with harmful functions of the hardware level, which cannot be destroyed by software. A flash drive with malicious content, submitted to the information protection service in time and analyzed by specialists in time, will make it possible to prevent, presumably, part of an APT attack. Therefore, it is not worth delaying the transfer of such findings. Some attacks on personnel of critical infrastructure facilities can also benefit from being implemented on a home computer. There they collect interesting information about the user and his passwords and look for loopholes to penetrate the workplace.

Fig. 1: Application GUI. Question screen

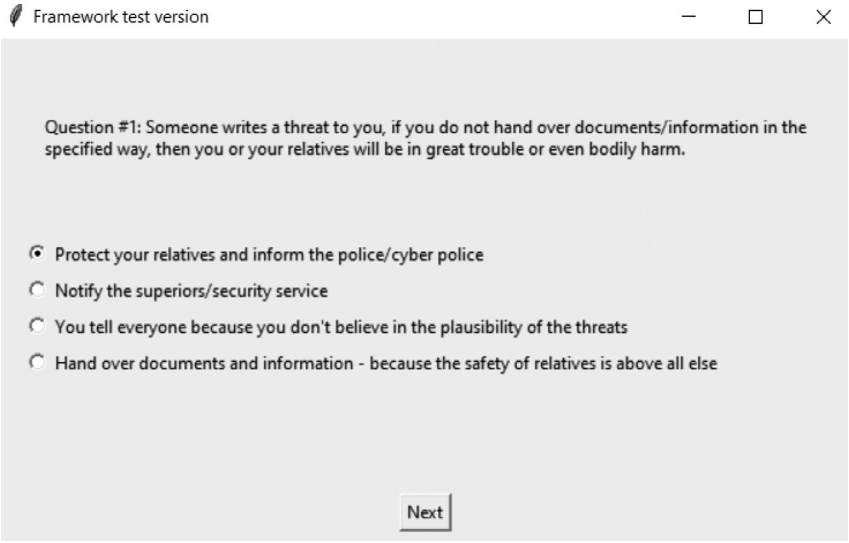


Fig. 2: Profile of the employee who answered the questions

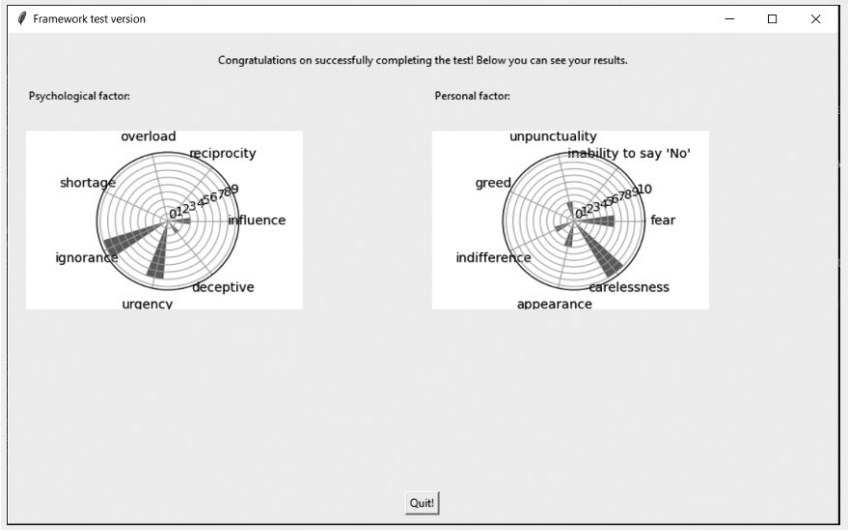
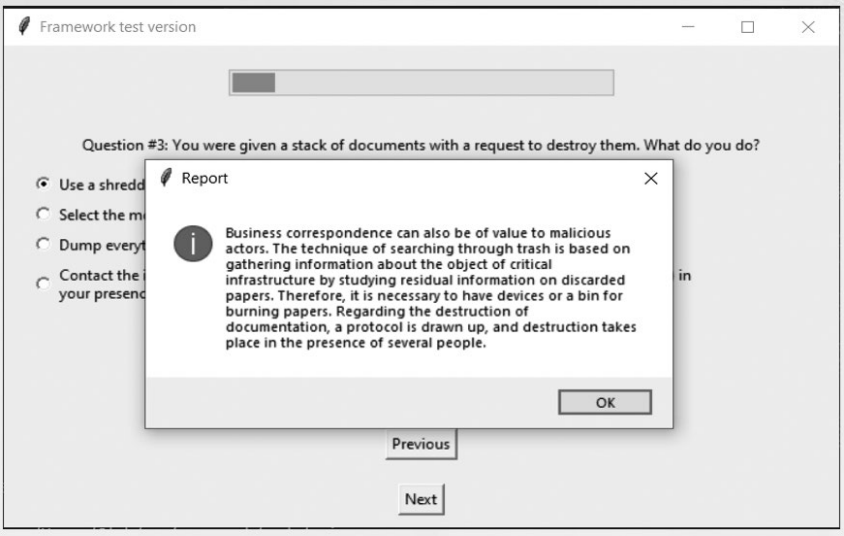


Fig. 3: Report with explanations on the issue



According to the proposed methodology, a survey of employees of companies classified as critical infrastructure of Ukraine was carried out (Ilin and Stopochkina, 2024), the research group consisted of randomly selected persons with an average and high level of knowledge in information technologies. According to the feedback of the respondents, it was established that the recommended length of the survey should not be too long. In the conducted survey, the length of the survey letter was 30 questions, 10 questions each on the social, socio-technical, and socio-physical vectors of influence. If the survey is longer, the respondents' attention is distracted, and the questions are not read carefully enough. Therefore, if it is necessary to conduct more detailed surveys, it is recommended to separate them in time.

The diagnostic and training module made it possible to identify a number of vulnerabilities, which mainly relate to the sphere of deceptive relations, vulnerabilities of a moral and ethical nature. In standard situations, the respondents reacted clearly and correctly, however, they did not always have a clear idea of how to act in non-standard situations. Thus, it should be noted the need to conduct not only standard trainings on countering cyber security threats but also special psychological trainings aimed at increasing resistance to social engineering attacks, which use subtle techniques of manipulation and exploitation of the victim's human vulnerabilities.

3.3 Linking Social Engineering Attacks to MITRE Techniques

Let us consider how social engineering can be used for the success of cyber attack techniques on critical infrastructure objects. Appropriate attention was paid to the issue in [19], however, we believe that it is possible to expand the provided information. We use the list of techniques from [30], and provide appropriate comments on the impact on the human factor (see Table 2).

Table 2: Correspondence of cyber attack techniques to methods of influencing the human factor

Number of the cyber attack technique	Name of the technique in the MITRE classification	Social engineering techniques that can be used in the implementation of the corresponding threats
T0800	Activate Firmware Update Mode	Exploitation through the social vector, persuasion, bribery, deceptive relations with employees, etc.
T0830	Adversary-in-the-Middle	Exploitation of the human factor by penetrating the territory of the organization, unauthorized use of equipment, involvement of insiders
T0878	Alarm Suppression	The human factor can be exploited through the socio-technical vector, and by violating the organizational principles of the security policy, by diverting the attention of the operator from his place of observation
T0802	Automated Collection	Socio-technical vector, use of malicious attachments, phishing.
T0895	Autorun Image	Physical, socio-technical vector. Replacing media with infected, harmful attachments.
T0892	Change Credential	Socio-technical vector, violation of the organizational regime.
T0858	Change Operating Mode	The implementation of the malware through socio-physical, socio-technical vectors
T0885	Commonly Used Port	Socio-technical vector, using data obtained through network intelligence using silent reverse proxy (Vlasenko, Stopochkina and Ilin, 2021)
T0884	Connection Proxy	Using a silent reverse proxy, sending fake links

(*Continued*)

Table 1: (Continued)

Number of the cyber attack technique	Name of the technique in the MITRE classification	Social engineering techniques that can be used in the implementation of the corresponding threats
T0879	Damage to Property	Physical vector, using the distribution of information about the object of critical infrastructure in networks. Publication of details of the operation of the object, the location of important premises, drawing attention to the object in social networks. As a result, missile strikes on critical infrastructure facilities (relevant for Ukraine in time of full-scale invasion) (Ovcharuk and Ilin, 2023).
T0809	Data Destruction	BYOD (Bring Your Own Device) policy permits, low level of employee education, socio-physical vector (use of third-party media, etc.). Using phishing lures via messaging and web vector.
T0811	Data from Information Repositories	Use of socio-technical vector, social vector to obtain access rights to internal and/or cloud repositories. Use of open repositories, unprotected due to inexperience of staff. Action through insiders
T0893	Data from Local System	Socio-technical vector use through the introduction of keyloggers, the use of insiders
T0812	Default Credentials	Exploitation of staff inexperience and inattention to credentials, and poor compliance with security policies
T0813	Denial of Control	Using ransomware in phishing messages
T0814	Denial of Service	The use of various types of malware distributed via the web and e-mail using phishing.
T0868	Detect Operating Mode	Sniffing, with penetration inside the object. Data theft of monitoring systems due to their weak security. Introduction of insiders, use of unauthorized software.
T0816	Device Restart/ Shutdown	The use of a specialized malware, distributed through a socio-technical vector
T0817	Drive-by Compromise	Web vector, the use of the "water holing" social engineering technique, when the popular web resource, used by organization, is successfully attacked first. Phishing lures

Number of the cyber attack technique	Name of the technique in the MITRE classification	Social engineering techniques that can be used in the implementation of the corresponding threats
T0819	Exploit Public-Facing Application	Accessing public services, contacts of a critical infrastructure object, exploitation of partnership and trust relations, obtaining guest accounts, access to public forums of a critical infrastructure object, placing malicious links there, injection attacks
T0890	Exploitation for Privilege Escalation	Elevation of privileges by means of a deceptive cosmetic vector in messages, impersonation of support and service services, impersonation of customers and partners of the object, impersonation of representatives of other branches
T0866	Exploitation of Remote Services	Social engineering attacks on remote services with which the company works.
T0822	External Remote Services	Obtaining access to remote services that are trusted on this critical infrastructure object. Gaining access to remote employee accounts through social engineering on family members, implanting of keylogger software on the victim workplace.
T0823	Graphical User Interface	Using a cosmetic vector, imitating the graphical interface of the programs that the user works with, replacing them with malicious ones. Distribution of maliciously modified updates, socio-technical attacks on the supply chain.
T0883	Internet Accessible Device	The introduction of IoT devices that are associated with the network of a protected facility, embedded with malware, will continue to serve as an entry point. Exploitation of the social factor and the "Trojan horse" technique, when air conditioners, coffee makers, electric photo frames or other smart household devices are given as a gift.
T0867	Lateral Tool Transfer	Using targeted phishing, emails that contain details that relate to a specific persons and may be of interest to them.
T0828	Loss of Productivity and Revenue	Delivering malware that will cause productivity losses using human factors.

(*Continued*)

Table 1: (Continued)

Number of the cyber attack technique	Name of the technique in the MITRE classification	Social engineering techniques that can be used in the implementation of the corresponding threats
T0849	Masquerading	Disguising harmful resources as harmless ones by copying the graphical interfaces of web resources and applications used by employees. Introduction of false links, introduction of software with a suitable interface but malicious functions through targeted phishing emails, through attacks on the supply chain, etc. Introduction of malicious software through dangerous links, and phishing emails with malicious attachments. Socio-physical vector, use of harmful carriers. Implementation of insiders with the possibility of access to the system.
T0838	Modify Alarm Settings	
T0821	Modify Controller Tasking	
T0836	Modify Parameter	
T0889	Modify Program	
T0801	Monitor Process State	Implementation of spy programs that carry out unauthorized collection of information from the monitoring system. Implementation can take place in a socio-technical, socio-physical way.
T0842	Network Sniffing	With the help of social engineering techniques, access to workplaces with administrator privileges, launching sniffing applications.
T0845	Program Upload	Obtaining access to the operator's workplace using social engineering techniques, which initiates appropriate actions. Introduction of malicious software that will perform unauthorized actions.
T0873	Project File Infection	Introduction of malicious software by tempting users to click on malicious links or open unverified attachments.
T0847	Replication Through Removable Media	Attacks on the supply chain: using developers, contractors, system operators, supplying them with removable media with embedded malicious functions. (Ilin, Rybak and Stopochkina, 2024)
T0848	Rogue Master	In the socio-technical aspect, the "master" may not be a substitute server, but the management, orders from which can be forged, for example, by using deep-fake
T0852	Screen Capture	Using social engineering methods to enter the facility, posing as guests, further spying, using special equipment with a high degree of magnification and photo-fixation.

Number of the cyber attack technique	Name of the technique in the MITRE classification	Social engineering techniques that can be used in the implementation of the corresponding threats
T0865	Spearphishing Attachment	Carrying out targeted social-engineering attacks through the mail service or messenger, sending a malicious attachment.
T0856	Spoof Reporting Message	Replacing the messages sent with similar ones - using technical means or a cosmetic vector.
T0862	Supply Chain Compromise	Social engineering attacks on employees of enterprises that are part of the supply chain. (Ilin, Rybak and Stopochkina, 2024)
T0857	System Firmware	Introduction of malicious code to the firmware, using the weaknesses of the security policy and employees of the manufacturing company
T0882	Theft of Operational Information	Actions through insiders, social engineering attacks on employees who have access to information
T0864	Transient Cyber Asset	Actions on behalf of the support service, repair services. Exploiting weaknesses in the BYOD policy.
T0863	User Execution	Manipulation with the aim of tempting the user to run a malicious program under the guise of a normal one. Malware in the documents sent, demanding to open the documents.
T0859	Valid Accounts	Obtaining information about account attributes, actions through a valid victim account.
T0887	Wireless Sniffing	Penetrating the wireless network coverage area using the human factor. Discovery of communication data, passwords.

** the socio-technical vector involves the use of human weaknesses in combination with the vulnerabilities of programs and equipment, or the use of technical means of increasing the attack.*
*** - the socio-physical vector involves the use of human weaknesses in combination with physical objects (for example, information carriers), features of the physical environment (for example, the conditions for access to premises, opening locks).*

As it can be seen, in order to exercise part of the influence, social engineers can act through persons from within the organization, whom we will tentatively call insiders.

The tool proposed in this paper can be modified according to the threat model of a specific enterprise of critical infrastructure, taking into account the most dangerous types of social engineering influences. This can be done by editing

the questions in the structured JSON file from where the diagnostic and training module reads the data.

3.4 Decision support module for requests. Operating principles and algorithm

To support decisions in case of requests to an employee of a critical infrastructure object who, for example, works in a call center or processes other external requests, a decision support module has been developed as part of the software package, which works according to an algorithm constructed on the basis of a modified SEADM algorithm. The proposed algorithm is distinguished by taking into account checks on the exploitation of factors that are especially dangerous for an employee of a critical infrastructure object and a shortened structure of the algorithm, which can be important in conditions of quick decision-making regarding the response to a request.

Factors taken into account in the algorithm:

1. *The employee's ability to make objective decisions at the moment*. The employee must independently assess his own psycho-emotional state and make a decision. In some cases, the condition can be assessed with the help of fitness bracelets with tracking indicators of physical condition.
2. *Sensitivity of the information being requested*. If the information being requested is confidential or critical to the organization, this may be a sign that someone is trying to gain access to the data through deception or other fraudulent methods.
3. *Violation of the information security policy or organizational rules* established in the organization. Such requests, which require the specified violations for their execution, are considered dangerous and must be rejected.
4. *The possibility of checking the authenticity of the requester*. In the case of requests that require confirmation of rights to access information, it is necessary to verify the person's attributes using reliable mechanisms.

The process of evaluating these factors is implemented through the program's interactive interface. When the operator doubts the legitimacy of the request and suspects a possible social engineering attack, he is directed to a series of clarifying questions. These questions allow you to gather additional information and help you determine what to do next.

The algorithm proposed in this paper (fig. 4) differs from the basic SEADM algorithm by the reduced number of questions to reduce the time of decision-making and by taking into account checks on the exploitation of factors that are especially dangerous for an employee of a critical infrastructure object:

After the assessment is completed, the system supports the operator in making one of three possible decisions:

1. Satisfy the request: if, after the verification, the request looks legitimate and does not cause suspicion.
2. Reject the request with notifying the security service: if the analysis indicates that the request is potentially dangerous and may pose a threat to the security of the organization.
3. Delegate the request; consult with other responsible persons: transfer the request to another employee who has more knowledge or authority to handle it, or share the responsibility with other competent colleagues. This may be necessary in cases where the request requires specialized knowledge or additional verification.

Questions in the system are formulated concisely and clearly, which makes it easy to use this method for all employees, regardless of their level of knowledge in the field of cyber security. This makes the system accessible and effective for a wide range of users.

3.5 Graphic user interface and architectural solutions of software package

The components of the software package are developed as an application in the Python programming language, using existing additional libraries to improve the user interface and data processing. These libraries include json, numpy, matplotlib, and tkinter.

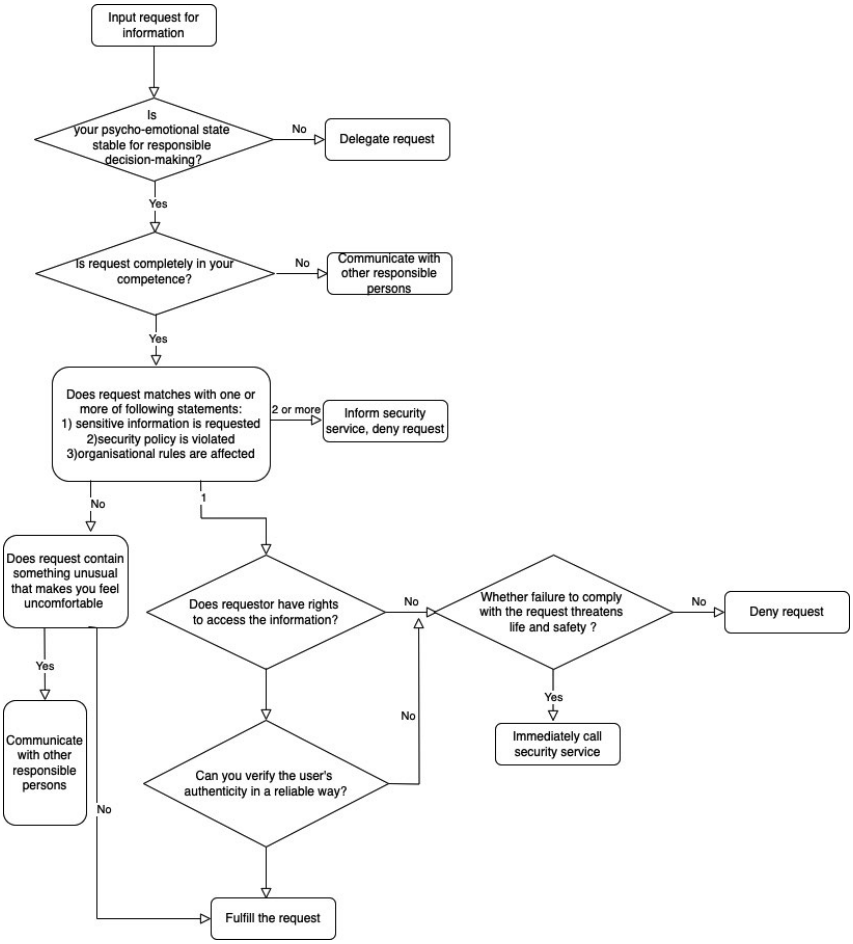
JSON library. This library is used to work with JSON format, where all the necessary data for the survey is stored. It provides a simple way of reading and writing data in a structured form, which facilitates convenience in their processing and analysis.

numpy library. The numpy library is used for data processing and analysis. It provides high-performance operations with multidimensional arrays and matrices and also offers a wide range of mathematical functions for working with these arrays. Using numpy allowed us to efficiently perform score calculations and data manipulation. This is especially useful when scoring answers and analyzing results.

matplotlib library. The matplotlib library is used to visualize the results. It allowed us to create charts for illustration of employee profile. This makes the data analysis process more visible and accessible.

tkinter library. Due to the fact that not all users know how to work with the console, the tkinter library was used to create the interface. It allowed us to create

Fig. 4: Algorithm scheme



a graphical user interface (GUI), making interaction with the program more comfortable and intuitive.

The program provides an opportunity to conduct questionnaires with automatic calculation of results. Each question in the questionnaire is pre-defined with a certain number of points for each answer option. Issues are also related to a certain environment, personal or psychological factors. This approach allows to systematize the collected data and carry out a detailed analysis of the results.

The data stored in the .json file has a clear and logical structure, which ensures its simple and efficient processing. This file contains fields for the text of the questions, answer options, assigned points for each answer, as well as metadata that indicate the relationship of the questions to certain categories of vulnerabilities of the respondent. This structure allows the program to easily interact with the data, automatically update it or add new questions without the need for changes in the program code.

4. Recommendations for increasing the resilience of personnel using the proposed solutions

Testing based on the tools proposed in the work can reveal situations when the user of the information system of a critical infrastructure object, an employee who works at a critical infrastructure enterprise, will show signs of vulnerability to social engineering attacks.

The first case that can be encountered is the presence of traits in the employee that can contribute to social engineering attacks. If these traits are personal, then it is advisable to work with the involvement of the company's full-time psychologist to eliminate or reduce the influence of these traits in working conditions. If this feature is generally social, i. e. found in anyone under certain conditions, efforts should be directed to improving the organizational components of the company's security, to prevent situations when it will be possible to exploit general social vulnerabilities of employees. For example, the uncertainty of how to act in force majeure situations is unacceptable at a critical infrastructure facility and is eliminated by providing detailed job instructions for various types of force majeure situations. Also, a useful solution is the use of the decision support module proposed in this work, which can be helpful in situations with some level of uncertainty.

The second case can be diagnosed when the employee belongs to one or more potentially vulnerable profiles of persons. This case must be verified, based on the observations and conclusions of HR (human resources) employees. It is also necessary to pay attention to the position held by the employee and the level of his access to sensitive data or facility systems. Depending on this information, the possibility of transferring the employee to a less critical area of responsibility, or conducting additional training with the involvement of a psychologist, should be considered.

Attention should be paid to the possible reasons for the presence of such traits in the respondent. If the cause is unsatisfactory social and labor conditions or an unhealthy working climate of the organization, it is necessary to work on eliminating these factors first of all. If the reasons for the appearance of these features

are subjective, it is necessary to observe the employee with the involvement of a full-time psychologist and HR employees, and then make a decision about the suitability of this employee to work at a critically important facility.

Recruitment testing cannot always objectively reveal traits that may lead an employee to become a conscious or unconscious accomplice of social engineering. Therefore, such testing should be carried out regularly, during the period of employee work, monitoring changes in their condition in the direction of human vulnerabilities.

Together with the above studies, the practice of conducting training to combat social engineering threats, as well as conducting penetration tests, with the identification of the readiness of the personnel of the critical infrastructure object to repel attacks, remains relevant. It will be useful for employees to take courses on emotional intelligence, which will allow a better understanding of the nature of certain emotions that lead to a vulnerable state and ways to prevent the formation of vulnerable states.

Creating favorable conditions for strict compliance with the provisions of the security policy, strengthening measures, and protection means is another necessary guarantee for the resistance of employees to attacks that exploit the human factor. The creation of transparent but protected communication, clear instructions for the employee, ergonomic and convenient interfaces of security devices, and ease of use are necessary conditions for achieving success in increasing the resistance of personnel to attacks on the object.

5. Conclusions

With the help of the proposed software package, it was found that the employees respond correctly to template situations, however, in the case of situations that contain elements of force majeure, deceptive relations, or receiving benefits, they may unconsciously act according to the plan of a social engineer. Thus, organizations should pay attention to trainings that affect exactly such non-standard situations that may arise at a critical infrastructure facility.

There is a connection between typical social engineering attacks and human vulnerabilities, on the basis of which it is possible to establish the resistance or vulnerability of a person to a certain type of cyberattacks that use the human factor. Therefore, to prevent these attacks, it is necessary not only to train personnel to be resistant to common social engineering attacks but also to eliminate existing vulnerabilities. Work on staff vulnerabilities can be carried out both with the involvement of psychologists and through organizational measures: maintaining a friendly atmosphere in the team, increasing employee motivation, and

implementing transparent communication mechanisms. Strict organizational requirements, a rigid management vertical without the ability to clarify management's orders, ask for explanations do not always contribute to the clarity of work, and may be the reason for the success of some social engineering attacks.

Even experienced employees are not always able to make objective decisions in case of non-standard situations, requests that lead to moral and ethical conflicts. In this case, the decision-making module proposed in the paper can be used to support decisions, which is aimed at helping an employee of a critical infrastructure object who often interacts with requests for the provision of important rights or information.

References

Anderson, Craig A. and Bushman, Brad J. (2002) 'Human aggression', *Annual review of psychology*, 53(1), pp.27–51. doi:10.1146/annurev.psych.53.100901.135231.

Arachchilagea, Nalin Asanka Gamagedara and Love, Steve. (2014) 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in human behavior*, 38, pp.304–312. doi:10.1016/j.chb.2014.05.046.

Barracuda (2019) Barracuda Phishline. Available at: https://assets.barracuda.com/assets/docs/dms/Barracuda_PhishLine_DS_US.pdf (Accessed: 29 July 2024).

Bezuidenhout, Monique, Mouton, Francois, and Venter, Hein S. (2010). 'Social engineering attack detection model: SEADM', *2010 Information Security for South Africa*, Johannesburg, South Africa, pp. 1–8. doi: 1-8.10.1109/ISSA.2010.5588500.

Bhakta, Ram and Harris, Ian G. (2015) 'Semantic analysis of dialogs to detect social engineering attacks', *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)*, Anaheim, CA, USA, pp. 424–427. doi: 10.1109/ICOSC.2015.7050843.

Bustamante, Eduardo E., Davis, Catherine L. and Marquez, David X. (2014) 'A test of learned industriousness in the physical activity domain,' International Journal of Psychological Studies, 6(4). doi: 10.5539/ijps.v6n4p12.

Cofense (2024) Phishing security awareness training. Available at: https://cofense.com/ (Accessed: 29 July 2024).

DataArt (2019) Social Engineering Test. Available at: https://www.dataart.com/services/security/social-engineering-test (Accessed: 29 July 2024).

Dupre, Kathryne E. and Barling, Julian. (2006) 'Predicting and preventing supervisory workplace', *Journal of Occupational Health Psychology*, 11(1), pp. 13–26. doi:10.1037/1076-8998.11.1.13.

Gallagher, Sean. (2016) 'Ransomware locks up San Francisco public transportation ticket mechines', *Ars Technica*, 28 November. Available at: https://arstechnica.com/information-technology/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/ (Accessed: 05 August 2024).

Ghafir, Ibrahim et al. (2018) 'Security threats to critical infrastructure: the human factor,' *The Journal of Supercomputing*, 74(10), pp. 4986–5002. doi:10.1007/s11227-018-2337-2.

Ilin, Mykola, Rybak, Oleksandr and Stopochkina, Iryna. (2024) 'Estimating the probability of attacks on key objects of the supply chain of critical infrastructure objects', *Theoretical and Applied Cybersecurity. Materials of All-Ukrainian scientific and practical conference (TACS-2024)*, Kyiv, May 2024, pp. 46–50.

Ilin, Kostiantyn and Stopochkina, Iryna. (2024) 'User profiling to increase the resilience of critical infrastructure personnel to cyberattacks that use the human factor'. *Information Technology: Computer Science, Software Engineering and Cyber Security*. (manuscript in preparation).

Kersten, Riccarda and Greitemeyer, Tobias. (2024) 'Human aggression in everyday life: An empirical test of the general aggression model,' *British Journal of Social Psychology*, 63(3), pp. 1091–1111. doi: 10.1111/bjso.12718.

Knapp, Deirdre J., Heggestad, Eric D., Young, Marc C. (2004) Understanding and Improving the Assessment of Individual Motivation (AIM) in the Army's GED Plus Program. Technical Review. Available at: https://apps.dtic.mil/sti/pdfs/ADA420227.pdf (Accessed: 05 August 2024).

KnowBe4 (2024) New-School Security Awareness Training. Available at: https://www.knowbe4.com/ (Accessed: 29 July 2024).

Krombholz, Katharina et al. (2013) 'Social engineering attacks on the knowledge worker,' *Proceedings of the 6th International Conference on Security of Information and Networks* [Preprint]. doi: 10.1145/2523514.2523596.

Lee, Robert M. et al. (2016) Analysis of the cyber attack on the Ukrainian power grid defense use case, NERC. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (Accessed 05 August 2024).

Liptak, Andrew. (2016) 'Hackers are holding San Francisco's light-rail system for ransom', *The Verge*, 27 November. Available at: https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni (Accessed: 05 August 2024).

Mataracioglu, Tolga and Ozkan, Sevgi. (2011) 'User awareness measurement for phishing attacks', *Information Management & Computer Security*, 19(4), pp. 315–327. doi: 10.48550/arXiv.1108.2149.

Mitnick, Kevin D. and Simon, William L. (2003) *The art of deception: controlling the human element of security*. New York : John Wiley & Sons, Inc.

MITRE (no date). ICS Techniques. Available at: https://attack.mitre.org/techniques/ics/ (Accessed: 05 August 2024).

Mouton, Francois et al. (2014) 'Social engineering attack framework', *Information Security for South Africa*, Johannesburg, South Africa, pp. 1–9. doi:10.1109/ISSA.2014.6950510.

Ovcharuk, Mykola and Ilin, Mykola. (2023) 'Models of denial of service attacks on cyber-physical systems', *Theoretical and Applied Cybersecurity*, 5(2), pp. 62–27. doi: 10.20535/tacs.2664-29132023.2.289459.

Parvez, Hanan. (2024) 'Am I selfish?' Quiz (Selfishness score). Available at: https://www.psychmechanics.com/am-i-selfish-quiz/ (Accessed: 05 August 2024).

PE Konsult Ltd. (2016) Personal Work-Related Responsibility Test. Available at: https://www.pekonsult.ee/testid/Vastutus.pdf (Accessed: 05 August 2024).

Sanger, David E., Krauss, Clifford and Perlroth, Nicole. (2021) 'Cyberattack forces a shutdown of a top U.S. Pipeline', The New York Times, 8 May. Available at: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (Accessed: 05 August 2024).

Shevchenko, Hrygorii, Stopochkina, Iryna and Babenko, Ivan. (2022) 'Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine', *Theoretical and Applied Cybersecurity*, 4 (1), pp. 108–117. doi: 10.20535/tacs.2664-29132022.1.

Test Partnership. (2023) TPAQ-45 Complete Profile, Full Report. Available at: https://www.testpartnership.com/samplereports/sample-report-personality.pdf (Accessed: 05 August 2024).

Tidy, Joe. (2021) 'Colonial hack: how did cyber-attackers shut off pipeline', *BBC*, 10 May. Available at: https://www.bbc.com/news/technology-57063636 (Accessed: 05 August 2024).

Vlasenko, Andrii, Stopochkina, Iryna and Ilin, Mykola. (2021) 'Methods of counteraction of bypassing two-factor authentication using reverse proxy', *Theoretical and Applied Cybersecurity*, 3(1), pp. 33–37. doi: 10.20535/tacs.2664-29132021.1.251299.

Zetter, Kim. (2014) *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Krzysztof Kaczmarek*, Mirosław Karpiuk**

Importance of Cybersecurity in the Healthcare System

Abstract: Technological advances bring both benefits and new threats to privacy and security; this is true of the healthcare sector in particular, which is one of those sectors that are the most vulnerable to cyberattacks. In this article, the Authors analyzed the importance of cybersecurity in the healthcare system by identifying the main threats, their mechanisms and their potential impact. The article also discusses the importance of security culture and the role of the human factor in countering cyberthreats. While verifying the hypothesis that an increase in digitalization causes the risk of cyberattacks to grow, the Authors conducted a literature analysis and case studies while pointing out the need for advanced protection mechanisms and continuous education of healthcare personnel to improve the security of healthcare systems. Furthermore, the present article highlights the importance of international cooperation and appropriate legal regulations in the fight against cyberthreats.

Keywords: healthcare, cybersecurity, Internet of Medical Things, phishing, education

Introduction

Technological progress results in changes occurring to the human living environment, bringing with it both an improved quality of life and challenges related to privacy or security in a broader sense. While providing new opportunities in areas such as education, entertainment, communication or healthcare, modern technology is also bringing with it new and previously unknown risks. This is particularly true of the development of Information and Communications Technology (ICT), which is an environment evolving so rapidly that the pace of change often exceeds the adaptive capacity of individuals, societies, and states. Simultaneously, public awareness of new threats, which is not keeping pace with ICT development, makes cyberspace an area that is the most frequently used for criminal activities. In view of the above, the consequences of negligence in the

* *Koszalin University of Technology in Koszalin, Faculty of Humanities, ORCID: https://orcid.org/0000-0001-8519-1667, Corresponding author's e-mail: krzysztof.kaczmarek@tu.koszalin.pl*

** *University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, ORCID: https://orcid.org/0000-0001-7012-8999, Corresponding author's e-mail: miroslaw.karpiuk@uwm.edu.pl*

area of cybersecurity may negatively affect every sphere of people's lives, and the level of threats is greater the higher the degree of digitalization of societies and states is. Consequently, ensuring cybersecurity is becoming one of the priority tasks for governments, businesses and organizations alike. At the same time, the global nature of cyberthreats means that their consequences most often extend beyond the borders of a single country (Skoczylas 2023: 99). This also applies to the healthcare system which, due to the volume and quality of data collected and processed, is one of those sectors that are the most vulnerable to cyberthreats.

In the era of the information society and of a state that relies heavily on ICT systems to function, where digital services are widely provided, cybersecurity takes on particular importance, as it not only enables uninterrupted social communication but also allows strategic sectors to be adequately secured, making the execution of numerous tasks more efficient. Cybersecurity offers protection against threats and thus ensures the normal functioning of the state on many levels, including an uninterrupted execution of tasks, as well as facilitating business operations (Karpiuk 2023: 190). What is one of the spheres of strategic importance for the state and society in particular is healthcare. The state must, as part of its policy, take into account not only expenditures on healthcare services but also on the protection of the ICT systems used for the purpose of these services.

In the case of a state that relies on ICT systems for its operations, intrusion into such systems may also take place through cyberattacks. In view of the need to ensure the proper functioning of the state, it is necessary to guarantee effective protection of critical infrastructure that is responsible for strategic sectors including public sectors. Effective protection of this infrastructure also involves securing ICT systems against cyberthreats (Czuryk 2023: 50). It needs to be emphasized that critical infrastructure also includes the healthcare system. In the province, the provincial governor is responsible for ensuring the effectiveness of measures aimed to protect public health, including counteracting infections and contagious diseases (Karpiuk, Kostrubiec 2024: 115–17).

In the source literature, what is the most frequently discussed issue, in the context of cybersecurity of the healthcare sector, is data security. Most researchers agree that the use of modern technology in healthcare has helped to improve the quality of services provided, while at the same time posing risks to the security of medical data (Sendelj, Ognjanovic 2022: 190). At the same time, it is noted that because one of the factors used during cyberattacks is the human factor, security culture, including cybersecurity culture, is widely discussed in the source literature (Uchendu, et al. 2021: 1). Simultaneously threats related to cybersecurity can have physical consequences, also in reality, even for people who do not directly use e-services (Włodyka, 2022: 203). The source literature also lists

types of cyberattacks that can be carried out against healthcare system organizations. These may include phishing, which involves obtaining credentials by manipulation or fraud (Wright et al. 2016: 1115). During the COVID-19 pandemic, ransomware attacks that encrypt data became a common form of attacks on healthcare entities (Muthuppalaniappan, Stevenson 2021: 1–2).

Analyses conducted by researchers also indicate that cyberattacks on health system actors, like all others, must somehow be motivated. This may be financial or political gain. However, in the case of a war, it may be about depriving as many people as possible of their lives (Coventry, Branley 2018: 49). Conversely, as the level of cyberthreats is increasing, organizations must be prepared to respond promptly (Hasan, et al. 2021: 12), and one of those factors that play a role in the level of cybersecurity is organizational culture (Berlilana, et al. 2021: 4).

The use of networked services in medicine based on, among other things, the Internet of Medical Thing (IoMT), forming part of the Internet of Things (IoT), allows an elimination of barriers to access time-critical services (Helser 2022: 1). Because IoMT is a combination of medical devices and IoT (Razdan, Sharma 2022: 775) and it involves management of large amounts of information, it is security that poses the biggest challenge (Natarajan, et al. 2023: 5).

Most studies indicate that the development of technology, including ICT, has created new opportunities for the provision, management and innovation of healthcare services; however, it is still bringing new challenges to operators in this area. At the same time, managing information security in the healthcare sector requires decent general knowledge both of information technology and the functioning of society.

The public sector constitutes a very important factor, one that allows effectively meeting the needs of society, be it local, regional, national or global communities. It is more and more frequently the case that public bodies perform their tasks using information and communications systems. These systems not only streamline the performance of public tasks but also make it possible to reduce their costs and reach a wider group of recipients in a relatively short period of time. In the light of the fact that the public sector constitutes not only an element stimulating the process of the provision of social services but also one enforcing certain behaviors of the participants of this process, appropriate management in this area will also be important (Karpiuk, Melchior, Soler 2023: 8). Good governance must also take place in the sphere of healthcare, which is increasingly using cyberspace to deliver services.

The main objective of this article is to analyze the importance of cybersecurity in the healthcare system and to identify the main threats, their mechanisms and potential impacts. The Authors also decided to seek answers to questions

concerning strategies, technologies and practices that may increase the level of digital security of medical systems and their protection against both current and future threats. At the same time, the research hypothesis is that an increase in the level of digitalization and the use of modern technologies in healthcare worsens the risk of cyberattacks, which requires an implementation of advanced protection mechanisms that combine both technical measures as well as continuous education and preparation of medical personnel.

In order to verify the hypothesis, the Authors chose to analyze the source literature, which provided a theoretical background to the research and allowed the current state of the research to be identified. The methodology used also includes case studies to illustrate the effects of cyberattacks on the healthcare system. Additionally, the Authors used quantitative and qualitative methods to assess the scale of the problem and to identify trends.

Mechanisms and potential consequences of cyberattacks on healthcare systems

More than 100 million people were affected by cyberattacks on healthcare providers in 2023; this is an increase of almost two and a half times compared to 2022 (Quinn 2024). At the same time, the current tense international situation and the aggressive policy pursued by Russia mean that there will be an increase in the number of Moscow inspired cyberattacks on healthcare entities. According to a report by the European Union Agency for Cybersecurity (ENISA), there has been an increase in the number of cyberattacks carried out by Russia and its affiliates against healthcare organizations and institutions since the beginning of 2023 (European Union Agency for Cybersecurity 2023).

These attacks constitute one element of the hybrid war being waged by Russia against the West, and the health system is particularly vulnerable to them due to the lack of experience and knowledge of the personnel in countering the threats posed by the attackers' use of military methods (Granholm, et al. 2023: 243). At the same time, attacks on medical targets aim to overload the system and are part of military tactics (Derrick, et al. 2023: 590). Simultaneously, lack of public awareness of the seriousness of the risks posed by information system security breaches poses a problem. This is also true of medical professionals, who are responsible for the life and health of many people. It should be noted at this point that knowledge of risks and awareness of their realness are not identical concepts. Although the most serious problem globally is gross underfunding of cybersecurity in the healthcare industry (Cartwright 2023: 1126), it is important to remember that it is the human being who constitutes the weakest link in cybersecurity. Indeed, while

technical measures to prevent cyberattacks possess a high level of effectiveness, there are none that could prevent irresponsible and risky actions taken by system users. Thus, there is a need for everyone who deals with data that should not be accessed by third parties to take responsibility for possible incidents (Loh Yee Ren, et al. 2020: 3).

All forms of cyberattacks, including those on medical entities, are linked by social engineering used in them, which is becoming increasingly sophisticated and personalized. Currently, the most common form of gaining access to medical systems is through phishing attacks. At the same time, a low level of knowledge and skills in recognizing potential threats can be observed among medical professionals, making them more vulnerable to socio-technical attacks (Weiner 2021). The digital skills deficit is also responsible for creating weak passwords that require no effort to guess them, making it easy for attackers to gain unauthorized access to medical systems. At the same time, the interoperability of medical systems means that an attack on one element of that system can lead to the compromise of the entire network (Ukyab, Beato 2024). This means that once a system has been infected with malware, it can infect further elements of that system without the user's knowledge or interaction (Szajstek 2024). It is also important to note that almost every successful cyberattack starts with a human error.

In May 2017, the global healthcare system fell victim to a massive cyberattack using the WannaCry ransomware affecting the National Health Service in the UK the most. The result was cancellation of thousands of scheduled medical procedures, rerouting of patients to other facilities and the blocking of access to patients' medical records. The attackers exploited a vulnerability discovered a year earlier in the Windows operating system and the fact that, by the time of the attack, a significant proportion of systems had been updated (Lessing n.d.). Another example includes LifeLabs, a Canadian diagnostics company, which was a victim of a major cyberattack in November 2019. The attack led to the leakage of personal data of ca. 15 million people. In this case, the attackers exploited a vulnerability in the company's security ("LifeLabs pays ransom"). Another example is the December 2022 phishing attack on the second largest integrated healthcare organization in the US: Highmark Health, The reason for the attackers' success was that one of the personnel members clicked on a malicious link received in an email, allowing the hackers to access his email. The impact of this attack affected around 300,000 people (McKeon 2023).

The examples presented above serve merely as examples yet they indicate that the vast majority of cyberattacks on health systems may have been effective due to a human error, and the findings indicate that the vast majority of these are examples of phishing (Alder 2024). However, it can be assumed that the use

of non-updated systems should also be considered as a human error. The same applies to security gaps in systems.

According to most security experts, the only solution that can significantly boost the resilience of systems to attacks is zero-trust cybersecurity, which consists of not trusting any information and data of the systems and a thorough verification every time access to resources is being granted (Yeoh, et al. 2023). This principle is valid across all industries and is effective even for individual users. However, it becomes particularly important in the healthcare system, as unauthorized access to, for example, the IoMT may result not only in the leakage of sensitive data but also be used to commit other crimes or even diversionary or sabotage activities. It is therefore important that anyone with access to medical systems is aware of this.

As regards attempts to unauthorizedly interfere with medical systems, the most relevant fact is that advanced digital tools such as artificial intelligence (AI), big data analytics or deep fake are employed for this purpose. Combining these with knowledge of social engineering and the personalization of cyberattacks means that it is not possible to offer complete protection against threats. However, these can be minimized when one assumes that any attempt to access data could potentially be an attempt to hack the system. This is all the more important as there is currently a war going on in cyberspace (Heromiński 2024: 206), and the healthcare system is particularly attractive to those actors whose aim is to destabilize the state.

The greatest risks are posed by those intrusions into ICT systems the effects of which pass unnoticed for a long period of time due to the fact that they were planned as early as at the design stage of these systems. In the case of AI, this can be an adversarial or manipulation of training data by introducing minor interference into the input data. This results in a misdiagnosis and an introduction of incorrect treatment if medical staff place too much trust in digital tools. A deliberately erroneously designed system can, for example, massively alter drug dosages under certain conditions or make small and almost imperceptible changes to medical records. The potential result is the death of many people and leading to social unrest, which undermines the capacity of the state. It seems important, therefore, that any training of medical staff on cybersecurity should also include content on achieving tamper resistance and elements of mechanisms for conducting hostile cyber activities. It is also important that those with access to medical systems only use secure devices and connections. It also needs to be noted that the healthcare system is not only about direct patient care but also about handling the distribution of medicines and managing medical staff. In the situation of a potentially possible military conflict with Russia, it should be taken into account that one of the first actions of this country will be cyberattacks on medical systems.

Conclusions and recommendations

In the face of rapid advances in ICT that exceed human adaptability, growing international tensions and the transfer of much social and professional activities online, sensitive sectors such as healthcare should receive particular protection. However, developing resilience to cyberthreats requires a holistic approach that encompasses education, development of new technologies, international cooperation and implementation of relevant legal regulations. At the same time, it is important to strike a balance between the efficiency of medical systems and the safety and guarantee of patient privacy (Ludvigsen 2023: 59).

Based on the analyzes carried out in this article, the hypothesis was positively verified that an increase in the level of digitalization and the use of modern technologies in healthcare worsens the risk of cyberattacks, which requires an implementation of advanced protection mechanisms, ones that combine both technical measures and continuous education and preparation of healthcare personnel.

The literature review confirmed that digitalization and modern technology indeed lead to an increased risk of cyberattacks in the healthcare sector. The analysis of cases such as the WannaCry attack on the NHS, the cyberattack on LifeLabs and the phishing attack on Highmark Health provided empirical evidence to support the hypothesis. At the same time, that quantitative data demonstrated a significant surge in the number of people affected by cyberattacks on healthcare systems, correlating with increased digitalization in the sector, qualitative methods identified trends and attack mechanisms, confirming that cyberthreats evolve alongside with technological advances.

In the context of education, it is advisable that the ability to recognize and defend against cyberthreats is built across society as a whole rather than in individual industries. However, every industry should train its personnel and upgrade their skills taking into account its own specificities and vulnerability to digital threats. Due to the evolution of technology, upskilling should constitute a continuous process. In the case of the healthcare sector, this is important both because of the development of medical technologies and the constant emergence of new digital tools, ones that can also be used by criminals.

Another element that may reduce the vulnerability of medical IT systems to threats is verification of compliance by healthcare professionals with security procedures. This applies especially to those who have access to medical data and have powers to modify it. Indeed, it cannot be ruled out that even a person with knowledge of cyberthreats and skills to counter them may at some stage make a mistake due to fatigue, malaise, routine or ignoring of procedures on a single occasion. This mistake may consist in using unsecured, also private, devices when

accessing medical systems. It is also important to remember that if access passwords are stored on a device and it is lost, unauthorized access to health systems is facilitated. It is also advisable to take into account, especially in the context of the huge number of employees in this sector, that there may be someone among them who, inspired by some third party, will deliberately carry out diversionary, sabotage or intelligence activities. At this point, it is important to indicate that a big data analysis allows data from medical systems to obtain information that is of value to hostile external actors.

In the future, further research should focus on developing innovative security methods and risk management strategies that are relevant to the specific needs of the healthcare sector. In this manner, it will be possible to create a more resilient and secure digital environment that effectively protects both patients and medical professionals.

Finally, it needs to be emphasized that the protection of cyberspace against threats is largely the responsibility of the administrative authority, which must also resort to measures of considerable severity to addressees (Kaczmarek, Karpiuk, Melchior 2024: 125). This protection also covers the healthcare system.

References

Alder, Steve, "Healthcare Data Breaches Due to Phishing", *HIPAA Journal* (6 January 2024), https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/> accessed 17 July 2024.

Berlilana, Tim Noparumpa, Athapol Ruangkanjanases, Taqwa Hariguna, and Sarmini, "Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cybersecurity Readiness and Technology Readiness", *Sustainability* 13/24 (2021), 1–20. https://doi.org/10.3390/su132413761.

Cartwright, Anthony James, "The elephant in the room: cybersecurity in healthcare", *Journal of Clinical Monitoring and Computing* 37/5 (2023), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5.

Coventry, Lynne, and Dawn Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward", *Maturitas* 113 (2018), 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008.

Czuryk, Małgorzata, "Cybersecurity and Protection of Critical Infrastructure", *Studia Iuridica Lublinensia* 5 (2023), 43–52. http://dx.doi.org/10.17951/sil.2023.32.5.43-52.

European Union Agency for Cybersecurity, *ENISA Threat Landscape: Health Sector* (July 2023). https://doi.org/10.2824/163953.

Granholm, Fredrik, Derrick Tin, and Gregory R. Ciottone, "The Complexities of Hybrid Warfare and the Impact on Tactical Emergency Medical Support", *Health security* 21/3 (2023), 242–245. https://doi.org/10.1089/hs.2022.0161.

Hasan, Shaikha, Mazen Ali, Sherah Kurnia, and Ramayah Thurasamy, "Evaluating the cybersecurity readiness of organizations and its influence on performance", *Journal of Information Security and Applications* 58 (2021), 1–16. https://doi.org/10.1016/j.jisa.2020.102726.

Helser, Susan, "Healthcare in the Balance: A Consequence of Cybersecurity", *Journal of The Colloquium for Information Systems Security Education* 9/11 (2022), 1–5. https://doi.org/10.53735/cisse.v9i1.145.

Heromiński, Maciej, "Wojna i konflikt w cyberprzestrzeni. Piąty teatr wojny" [War and conflict in cyberspace. The fifth theatre of war], *Przegląd Bezpieczeństwa Wewnętrznego* 30 (2024), 185–211. https://doi.org/10.4467/20801335PBW.24.008.19610.

Kaczmarek, Krzysztof, Mirosław Karpiuk, and Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data", *Prawo i Więź* 3 (2024), 117–135. https://doi.org/10.36128/priw.vi50.

Karpiuk, Mirosław, "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity", *Studia Iuridica Lublinensia* 2 (2023), 189–201. http://dx.doi.org/10.17951/sil.2023.32.2.189-201.

Karpiuk, Mirosław, Jarosław Kostrubiec, "Provincial Governor as a Body Responsible for Combating State Security Threats", *Studia Iuridica Lublinensia* 1 (2024), 107–122. http://dx.doi.org/10.17951/sil.2024.33.1.107-122.

Lessing, Marlese, "Case Study: WannaCry Ransomware", *SDxCentral* (n.d.) <https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-wannacry-ransomware/> accessed 17 July 2024.

"LifeLabs pays ransom after cyberattack exposes information of 15 million customers in B.C. and Ontario", *CBC News* (17 December 2019) <https://www.cbc.ca/news/canada/british-columbia/lifelabs-cyberattack-15-million-1.5399577> accessed 17 July 2024.

Loh Yee Ren, Amos, Chong Tze Liang, Im Jun Hyug, Sarfraz Nawaz Brohi, and N. Z. Jhanjhi, "A Three-Level Ransomware Detection and Prevention Mechanism", *EAI Endorsed Transactions on Energy Web* 7/26 (2020), 1–7. https://doi.org/10.3390/su132413761.

Ludvigsen, Kaspar Rosager, "The Role of Cybersecurity in Medical Devices Regulation: Future Considerations and Solutions", *Law, Technology and Humans* 5/2 (2023), 59–77. https://doi.org/10.5204/lthj.3080.

McKeon, Jill, "Highmark Health Suffers Phishing Attack, 300K Individuals Impacted", *HealthITSecurity* (6 February 2023) <https://healthitsecurity.com/news/highmark-health-suffers-phishing-attack-300k-individuals-impacted> accessed 17 July 2024.

Mirosław Karpiuk, Claudio Melchior, and Urszula Soler, "Cybersecurity Management in the Public Service Sector", *Prawo i Więź* 4 (2023), 7–27. https://doi.org/10.36128/PRIW.VI47.751.

Muthuppalaniappan, Menaka, and Kerrie Stevenson, "Healthcare cyberattacks and the COVID-19 pandemic: an urgent threat to global health", *International Journal for Quality in Health Care* 33/1 (2021), 1–4. https://doi.org/10.1093/intqhc/mzaa117.

Natarajan, Rajesh, Gururaj Harinahallo Lokesh, Francesco Flammini, Anitha Premkumar, Vinoth Kumar Venkatesan, and Shashi Kant Gupta, "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0", *Infrastructures* 8/22 (2023), 1–18. https://doi.org/10.3390/infrastructures8020022.

Quinn, Neal, "Cyberattacks On Healthcare Soar: What Lies Ahead In 2024", *Healthcare Business Today* (14 January 2024) <www.healthcarebusiness-today.com/cyberattacks-on-healthcare-soar-what-lies-ahead-in-2024> accessed 14 July 2024.

"Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double" (28 February 2024) <https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf> accessed 15 July 2024.

Razdan, Sahshanu, and Sachin Sharma, "Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies", *IETE technical review* 39/4 (2022), 775–788. https://doi.org/10.1080/02564602.2021.1927863.

Sendelj, Ramo, and Ivana Ognjanovic, "Cybersecurity challenges in healthcare", in: John Mantas, Arie Hasman, Reinhold Haux, eds., *Achievements, Milestones and Challenges in Biomedical and Health Informatics* (IOS Press, 2022), 190–202. http://dx.doi.org/10.3233/SHTI220951.

Skoczylas, Dominika, "Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe" [Cyberthreats in cyberspace. Cybercrime, cyberterrorism and network incidents], *Prawo w Działaniu* 53 (2023), 97–113. https://doi.org/10.32041/pwd.5306.

Szajstek, Daniel, "Oprogramowanie złośliwe – robak komputerowy" [Malware: a computer worm] (9 May 2024) <https://www.wojsko-polskie.pl/woc/articles/publikacje-r/oprogramowanie-zlosliwe-robak-komputerowy> accessed 16 July 2024.

Tin, Derrick, Dennis G. Barten, Fredrik Granholm, Pavlo Kovtonyuk, Frederick M. Burkle, and Gregory R. Ciottone, "Hybrid warfare and counter-terrorism medicine", *European Journal of Trauma and Emergency Surgery* 49/2 (2023), 589–593.

Uchendu, Betsy, Jason R. C. Nurse, Maria Bada, and Steven Furnell, "Developing a cybersecurity culture: Current practices and future needs", *Computers & Security* 109 (2021), 1–23. https://doi.org/10.1016/j.cose.2021.102387.

Ukyab, Kesang Tashi, and Filipe Beato, "Healthcare pays the highest price of any sector for cyberattacks - that's why cyber resilience is key", *World Economic Forum* (1 February 2024) <www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key> accessed 15 July 2024.

Weiner, Stacy, "The growing threat of ransomware attacks on hospitals", *AAMC* (20 July 2021) <https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals> accessed 15 July 2024.

Włodyka, Ewa Maria, "Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa" [Ready – steady – go? A contribution to the discussion on local government cyber security readiness], *Cybersecurity and Law* 1 (2022), 202–219, https://doi.org/10.35467/cal/151828.

Wright, Adam, Skye Aaron, and David W. Bates, "The Big Phish: Cyberattacks Against US Healthcare Systems", *Journal of General Internal Medicine* 31 (2016), 1115–1118. https://doi.org/10.1007/s11606-016-3741-z.

Yeoh, William, Marina Liu, Malcolm Shore, and Frank Jiang, "Zero trust cybersecurity: Critical success factors and A maturity assessment framework", *Computers & Security* 133 (2023), 103412. https://doi.org/10.1016/j.cose.2023.103412.

Andrzej Pieczywok*, Ewa Maria Włodyka**

Man and Society and the Development of Digital Humanities: Selected Issues

Abstract: The aim of the present article is to prepare man for life in society by equipping them with the necessary life and professional competencies in the context of the development of digital humanities. The article depicts the essence of man in society; it draws attention to dilemmas in human activities; it presents the importance of humanities in human development, in issues of upbringing and education. The Authors devote a lot of attention to the use of knowledge in the workplace as well as to an adaptation of employee competencies to changing conditions in the organization's environment. The topicality of the problem is evidenced by an increasing number of publications devoted to the issue of the turbulent environment on the one hand and issues of new digital technologies on the other. In addition, issues of artificial intelligence as an element of public policies will be addressed. In the context of the development of humanities and humanities being influenced by artificial intelligence, a survey of the desired digital skills for the future of professional work will be carried out. The article considers possibilities of taking optimization measures to enhance human knowledge, skills, and competencies in the area of digital humanities. The Authors formulate their own construction of the importance of digital competencies for civil society. Preparing to be an informed and active member of society in the area of information security appears to be as important as imparting knowledge in mathematics or physics. The aim of the pilot study is to better understand the needs of the labor market regarding the requirements of employers in the context of the development of new technologies. A study was conducted on the expectations of employers in Poland regarding the level of digital skills and knowledge of artificial intelligence in employees by way of an anonymous survey containing 6 closed substantive questions; the answers were collected in July 2024.

Keywords: digital humanities, work of the future, competences, new technologies, labour market, public policies

* *Professor, PhD, University of Kazimierz Wielki in Bydgoszcz, Faculty of Political Science and Administration, ORCID: https://orcid.org/0000-0002-4531-0630, Corresponding author's e-mail: a.pieczywok@wp.pl*

** *PhD, Koszalin University of Technology in Koszalin, Faculty of Humanities, ORCID: https://orcid.org/0000-0002-8229-342X, Corresponding author's e-mail: ewa.wlodyka@tu.koszalin.pl*

Introduction

Contemporary man is confronted with the need to fulfil numerous social, professional and educational roles, resides in various spaces, often adapting to new circumstances, and makes numerous decisions in situations of uncertainty and risk. Risks and conflicts constitute an attribute of people's lives, the functioning of organizations, states, and societies. There is a widespread belief that almost everyone wants to feel safe. Raising people's awareness of existing risks, through proper upbringing and education, helps to avoid a 'catastrophe', and thereby enhances their psychological wellbeing.

A person's relationships with his or her environment influence their sense of security as that person shapes the conditions in which he or she functions, which is strongly emphasized in the following definition: "Personal security consists in creating for man (a person, a human individual) such multiple conditions of existence which, if properly consumed by them, will ensure them complete personal development: self-realization or, in other words, continuity of existence as a specific individual." (Kolodziejczyk 2009: 140).

The modern world is a world of dynamic changes in almost any sphere of human existence; it also involves numerous threats. Contemporary threats and conflicts are mainly of a 'hybrid' nature while taking place in different dimensions (Kuliczkowski 2016: 10). It is worth recalling here Alvin Toffler's views: "The scientific and information revolution that is currently sweeping the world has completely changed the most important goals of conflicts. The most important emphases of competition have shifted from the struggle for material resources to the struggle for intellectual and spiritual resources. What is at stake is human consciousness. It is a war without front lines. It is the human mind that has become a battlefield." (Toffler 1985: 501–4).

The world created by man is getting out of their control and gives rise to many previously unforeseeable threats to its creator, turning not only against man but also against nature. It is becoming dangerous and poses threats to the continuation (of nature), the continuation of life (of the organic world) and the survival (of man and social life, values and ethical norms cherished for centuries). It is putting pressure on science, it deepens its decentralization and dehumanizes it, dividing it into natural sciences, technical sciences and humanities (Bakywok 2018: 194).

When analyzing man and society in the context of the development of digital humanities, it is worth realizing that for centuries their main sources have been in nature itself, in the untamed forces of nature. Furthermore, man as such posed (and is still posing) a threat to others. Through the use of various tools and techniques, man has been using coercion and force, the most spectacular expression

of which has been the wars that man has initiated and waged. The third, historical source of threats and dangers is a specific social order (more precisely: political systems and forms of state power), which did not provide man with adequate and safe standards of living. In the context of digitalization, it is the human being who is identified as the weakest link in cyber security systems (Włodyka 2022: 2016). In the face of evolving information technologies, the issue of 'the weakest link', represented by end users, is gaining importance. (Karpiuk, Melchior and Kaczmarek 2024: 117). And this link is usually the human being - hence the importance of the symbiosis of the human being and the humanities in the digital face.

Zygmunt Bauman ponders how it is possible that, despite being the most technically equipped generation in the history of mankind, we are more intensely than ever plagued by feelings of insecurity and helplessness. According to him, ours is an age of anxiety, in which people feel threatened, insecure and frightened, they easily succumb to panic and more fervently than ever offer their attention to everything connected with a sense of certainty and security (Bauman 2008).

New technologies are playing an increasingly important role in providing security. In today's world, where many processes take place online, threats of cybercrime, data theft or hacking attacks are becoming more frequent. These threats are being used to harm objects available both in cyberspace and in the real world, also to support criminal and terrorist activities. Nowadays, cyberspace represents the fifth dimension of warfare[1], offering rich opportunities for offensive action. The dynamic qualitative development of threats (being manifested, for example, in the creation and spread of hitherto unknown new types of malware) limits the possibilities of defense to a large extent to reactive actions. ICT devices, which allow communication with other users of cyberspace from anywhere at any time, are readily available, and the cost of purchasing them is low. Knowledge of 'how to harm' can easily be obtained online (Witecka 2014).

As experience in recent years has shown, attacks in the cybersphere can be politically and religiously as well as business motivated. Increasingly, cyber attacks are targeting critical infrastructure elements, becoming a tool of blackmail in the hands of organized crime. Therefore, the development of modern technologies is key to ensuring information security. They make it possible to respond quickly to threats, secure data and effectively protect against attacks. Consequently, investment in the development and implementation of new solutions is essential to ensure security in today's digital world. Additionally, these solutions should not be implemented at the micro level of a country but at the macro level as systemically

1 The others include: air, sea, space and land.

adopted comprehensive solutions in the form of public policies. Within the framework of a democratic state under the rule of law, these policies should conform to deliberative standards, be subjected to diverse community consultations, as well as be systematically and in succession implemented and evaluated (Chałubińska-Jentkiewicz and Karpiuk 2015: 73).

While valuing the topic finally taken up, we intended the issues considered in this article to fall within the sphere of promoting the idea of humanity and digital humanities understood, following Bogdan Suchodolski, as: "[…] a certain view of the world and a certain attitude of man (which) had, of course, its historical genealogy, but always transcended the historical boundaries of the epochs that developed it, becoming a permanent and universal good of the human world, elevated above the variability and limitation of the times, although rooted in their conflicts and hopes. Conceived in this manner, humanism constitutes an attempt to answer the question about the meaning of human life, an attempt to define the tasks of human action in this world in which they live; it is a measure of human responsibility for acts undertaken or omitted in relations between people and in society, and is thus a voice of conscience watching over the human community." (Suchodolski, Wojnar 1988: 13).

This paper seeks to answer the following research questions, based on the existing literature and the results of our own research:

a) RQ1: What is the level of knowledge of business entrepreneurs regarding public policies on artificial intelligence?
b) RQ2: what are the concerns and expectations of businesses entrepreneurs over the next five years regarding the ICT skills of their workforce?

We used a mixed methods approach, applying research tools and techniques being specific to social sciences: content analysis, legal analysis, desk research and CAWI. The aim of the pilot study is to better understand the needs of the labor market concerning the requirements of employers in the context of the development of new technologies. The survey on the expectations of employers in Poland regarding the level of digital skills and knowledge of artificial intelligence by employees was conducted in an anonymous survey containing six closed substantive questions. The answers were collected in July 2024.

Importance of digital humanities in human development

The process of globalization, including communication techniques, has almost completely erased differences in access to information and to knowledge, while at the same time allowing people to become familiarized with other different

countries and lands, cultures and customs, religions and traditions. All of this makes it necessary for communities to systematically gain further education, develop and change their professional profiles. ontrary to the opinions of those who believe that industrial civilization is dehumanizing and destroys the quality of life, it is clear that it is in the highly industrialized societies of the West that our opportunities for education and self-expression, as well as equitable satisfaction of spiritual and material needs have reached their highest levels (Harari, 2018, p. 73). Digital humanities is a prospective research field, one that indicates the importance of an interdisciplinary approach to the equivalent development of new technologies on the one hand and, on the other, the development of social and digital human skills with their ubiquity of application. The main cognitive competencies of the 21st century include critical thinking, creativity and problem solving (Wechsler et al. 2018). Critical thinking involves self-disciplined thinking during which an individual evaluates, synthesizes and interprets relevant information related to a situation (Hyytinen, Toom and Postareff 2018), and effective argumentation involves analyzing alternatives in relation to one's goals and justifying conclusions, both of which can be included in scoring criteria (Newman, Webb and Cochrane 1995). These facts are undeniably relevant to humans and their cognitive abilities in the face of the exponential growth and ubiquity of access to artificial intelligence.

The process of actively seeking humanistic conditions for human life and development has always been close to the development of digital human resources.

Digital humanities emerged in academia and gained popularity at the turn of the 20th and 21st centuries, but the current name was perpetuated only at the beginning of this century. There is still no permanent definition of digital humanities due to the constant expansion of the field in which they operate. It may even be the case that they will not obtain any final definition because the term 'digital' will simply lose its meaning. It is becoming increasingly clear that every science, regardless of the discipline, uses digital tools and methods. What is significant about the doctrinal approach to digital humanities, however, is that critical studies of technology and its applications, innovative methods and tools for humanities, and the transformation of knowledge production are the main focus areas of digital humanities. Additionally, they emphasize increasing public impact on social justice, ensuring sustainability in the field and digital modes of production, and accelerating the radical transformation of broader systems of cultural knowledge production (Fenlon, Frazier and Muñoz 2024).

The popularity of digital humanities was driven not only by the development of technology but also by the position of humanities as such in the field of science. Humanists found it worthwhile to adapt digital technology tools to their needs,

which broadened the field of research and allowed the results to be presented to a wide audience in an attractive manner.

Digital tools have changed the manner in which scholars work. In particular, their influence has also become noticeable on the work of humanists. New research methods have emerged, the range of ways of presenting their results has expanded, and methods of data acquisition and scientific communication have radically changed (Buczyńska-Łaba, Krasińska 2016: 24).

After all, digital humanities have been developing in Poland for a relatively short period of time, which is a good moment for information professionals to become involved in its development. So far, this topic has not found much attention among researchers, although it is very important for shaping the profession of information professionals. To date, the subject of digital humanities has already been covered by many studies, ones that extensively deal with the related issues.

The society of our decade is referred to as an information society. This is confirmed by the phenomenon of new media which, based on the features of virtuality, the hypertextuality of the content of the novel or of the text as such, move into a different, i.e. digital dimension of communication. Hence the textual chaos, the question of who is the author and who is the reader, are present on the Internet. A peculiar supermarket thus also has its unveiling on the global web.

In a society of risk, the individual must possess specific skills and abilities in order to efficiently function in it. "Of vital importance here is the ability to anticipate dangers, to tolerate them, to cope with them in a biographical and political sense." (Beck 2004: 98). Dealing with anxiety in a society of risk is, for the time being, rather an individual matter; however, as Ulrich Beck predicts: "This increasing necessity to deal with uncertainty will sooner or later give rise to new demands to public institutions in the fields of education, therapy and politics. In a risk society, dealing with fear and uncertainty becomes a biographically and politically basic civilizational qualification." Today, man must be able to calculate the risks, opportunities and dangers that they are being confronted with.

Among the specific characteristics of new media, the following are particularly noteworthy: interconnectedness; access by individual users who can be both senders and receivers; interactivity; multiple uses and openness; ubiquity; spatial indeterminacy; and delocalization (Berkeley 2005: 77). According to Lev Manovich, new media is, among other things, a novel approach to the reality around us, resulting from the possibilities opened up by all new technologies at their early stages of development (Manovich 2006: 119–20). New media differs from its predecessors by the shift from mass communication towards networked communication, fragmentation and further obliteration of the media institution, and the weakening of social control.

However, many, especially young users do not understand the technologies they use. Many, for example, fail to perceive the problem of media broadcasters deliberately sending out falsified messages that lead to misleading and misinterpreted content. This unfamiliarity with the workings of modern media is worrying, if we remember that they are an extension of the human brain, increasingly altering our consciousness and dictating directions in humanity development (Morbitzer 2007: 334).

It also seems important to address the issue of manipulation in media. Children and young people are a group of media users who are particularly vulnerable to manipulation. Threats posed to young internet users by the web are usually associated with the problem of pedophilia or other forms of action by adults against children. These issues remain relevant; however, in recent times, with an increasing accessibility of new media to children and a wider range of opportunities these media offer, their peers are also becoming a serious threat to the youngest.

Computer games and the internet are entering private homes at an alarming pace; they are the latest and most potent means of leading to depersonalization. Thanks to computers and the internet, yet at the expense of closer family ties, people are becoming members of the global village. As technology is taking over more and more activities previously performed by humans, the ability of individuals to influence the course of events and the opportunities for face-to-face contact between people are diminishing.

The challenge posed to us in the 21st century by information technology and biotechnology is arguably far greater than the challenge posed by steam engines, railways and electricity in a bygone era. Given the immense destructive power at the disposal of our civilization, we cannot afford more failed models, world wars and bloody revolutions. This time, such failed experiments could end in nuclear wars, monstrous genetic modifications and a total disintegration of the biosphere. Therefore, we must do better than when we faced the Industrial Revolution (Harari 2018: 58).

Importantly, the digitalization of societies is reflected in the approach accepted by governments and the public policies they create. In the case of the European Union, this concerns EU standards, policies or normative solutions adopted within the Member States.

Digital competencies training for employees

In the face of the numerous risks and uncertainties of human existence residing in the various spaces of their life, the fundamental question arises: how to avoid or cope with these? This question often comes down to the quality and effectiveness

of a person's education so that he or she could effortlessly make use of modern information and communication technologies. Hence, in view of the many different professional competences of an employee, digital competences play an important role. Digital competences, along with reading, writing, mathematical and linguistic skills, constitute a set of fundamental skills for modern man.

When the right to the Internet starts to be counted among the fourth generation of human rights, digital competencies become a primary skill: one that is indispensable at work, in dealing with banks, with offices: arranging matters without leaving home, or with relatives, communicating with them using modern technologies. Without a certain degree of proficiency with computers, the internet, software, the ability to search and critically evaluate information found, and without an ability to use these competencies at work, study and private life, such a person is doomed to exclusion.

Digital competencies have been of interest to researchers since the advent of technology in social life. Digital competencies can be considered to be the result of knowledge, skills and attitudes that enable people to live, learn and work in a digital society, i.e. a society that uses digital technologies in everyday life and work. These mostly include digital competencies (encompassing an efficient use of computers, the internet, software, etc.), information and communication competencies (e.g. searching information, selecting information, communicating at a distance, etc.) and functional competencies (the use of such skills in various spheres of human life: school, work, finance, social relations, etc.).

It needs to be stated that professional work is increasingly dependent on technology, digital solutions and the internet. The level of digital competencies will affect the competitiveness, efficiency as well as innovation of businesses. Therefore, employers are increasingly looking for those employees who will not only understand the need to function in the digital world but, above all, be able to use the tools of new technologies. Digital competencies are also becoming essential in personal and social life.

Tackling the digital skills gap is a necessity that is no longer being talked about only at the national but also at European level. Possessing these competencies also means being able to use technological solutions (frequently, facilities) on a daily basis.

Digitalization is increasingly affecting education. Education is one of the most important forms of digital competencies education among the workforce. However, adequate digital competencies education requires the school to be adapted to this type of education. Validation of digital competencies seems to be necessary in terms of examining the resources available for business development but also in order to retain an employee in the organization, for whom

improving competencies is often a reason to stay with the company. Specifically, three paths for acquiring digital competencies are proposed to employees: in-company courses or training, external training and self-education.

Education is, in a sense, a form of scientific conversation and, although, as Dawid Juraszek claims, this "[…] conversation (face to face, using distance communication, in black and white) will show us the route, give us binoculars, even lace up our shoes, but it will do nothing without our action […]" (Juraszek 2020: 171), we also believe that it will motivate us to act, make sound decisions and apply effective solutions, and thus will enable us to create positive relationships with the environment which we live in.

Education is an important area of social life. It takes place at a specific time and is directed towards the future. It is a very broad concept; in a broad sense, it may mean "the totality of diverse influences and systematic cultural formation of people" (Łomny 1996: 44) or, as Irena Wojnar proposes, an awakening in the individual of the need to know and feel the world and values and an inspiration of creative activity (Wojnar 1996: 25).

The education and upbringing of people is certainly one of the most important activities in human life. After all, the development and progress of societies depends above all on a good preparation of young people for functioning in society and making changes to existing systems.

Digital educational resources should correspond to the requirements of the teaching methods and forms used by teachers. In order to make full use of digital resources, teachers need ideas for lesson plans and inspiration for curriculum development using them. The main purpose of using digital educational resources should be an intended didactic goal in the teaching process.

In this context, creation of appropriate platforms for making digital educational resources available is also a key issue. Different functionalities and usage models of digital resources have an impact on infrastructural and hardware requirements. Activities to improve teachers' competencies should also be adapted to them.

What is a very interesting initiative is the creation of online digital libraries of educational resources, which may take various forms, e.g. these can be themed libraries of resources, subject-related libraries, and libraries adapted to educational levels or stages.

Digital schooling therefore offers a response to the need to build the workforce competences of the future in the context of the needs of the contemporary labor market. The digitalization of education takes many forms and it also influences the way contemporary vocational education is perceived in general. Digital education is a state of the awareness of perceiving education in the context of goals, time, place and space, and the development needs of contemporary society.

This state is determined by the legal, technological and social framework. Learning about it, implementing it and finally being able to evaluate its benefits is a long-term process. Digital education means digital educational standards, educational models, tools or educational spaces.

As a result of the current considerations, the following question arises: how is one to plan and conduct lessons with the use of new technologies so that it is not merely a one-time and attractive activity but an effective teaching process? It seems that the key role in this process should be played by teachers, whose high level of digital competencies will ensure a high standard of education with the use of modern technologies.

However, the level of digital competencies is not only the domain of teachers and the generation Z that is entering working age. They are reflected in the aforementioned area of EU regulation. Although EU Treaties do not specify provisions on information and communication technologies (ICT), the EU can act within policy areas based on the Treaty on the Functioning of the European Union of 13 December 2007: consolidated version (OJ C 202, 7.6.2016, pp. 47–360). The EU aims to empower businesses and people for human-centered, sustainable and more prosperous digital future, which fits with the foundations of the idea of digital humanities. The EU is pursuing a human-centered and sustainable vision of the digital society throughout the digital decade to empower citizens and businesses. As early as in the 2010 European Digital Agenda, with reference to the Lisbon Strategy, emphasized that ITCs play a key role in achieving the EU's goals. The European Digital Agenda 2020–2030 (Decision EU 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance), PE/50/2022/REV/1) takes these developments into account. Its priority is to establish secure digital spaces, ensure fair competition in digital markets and strengthen Europe's digital sovereignty, in line with the dual digital and ecological transformation. In 2021, the EU also introduced a digital compass setting four targets for 2030, including those in the area of 'skills': at least 80% of all adults should possess basic digital skills and 20 million ICT professionals should be employed in the EU, with more women taking up such jobs (European Parliament 2024).

Setting of targets is followed by their evaluation: the European Union monitors the state of digitization in each country. The results form the basis for the Digital Economy and Society Index (DESI), which makes it possible to compare the level of digitization in different countries. According to DESI research, only 44% of Polish people aged 16–74 possess basic digital competencies (Carretero et al. 2017: 3). DigComp 2.2 is another iteration of the European Digital Competence Framework for Citizens (DigComp), which has been there for ten years now.

This framework makes it possible to systematize areas and levels of competence, as well as to set up systems to measure and certify these. In addition, the DigComp framework needs to be periodically modified and adapted to the current state of digital technologies[2], and EU citizens should also adapt their knowledge, skills and attitudes to technological change (ibid.). DigComp 2.2 provides grounds for the implementation of EU policies in the area of digital competencies of its citizens. Digital Competencies are therefore of a special nature, as they directly contribute to and influence the process of acquiring other key competencies in everyone's life. They are linked to a number of skills that all the citizens of 21st century Europe should possess in order to ensure their active participation in social and economic life.

ITCs are a relevant concept for yet another reason with the emergence of artificial intelligence technology[3]. As early as in 2020, the White Paper on Artificial Intelligence (White Paper on Artificial Intelligence: a European approach to excellence and trust English COM(2020)/ 2020) highlighted the key role of AI in modern society and foresaw its social and economic benefits in all sectors. The EU Parliament in turn adopted regulations for its use in the Artificial Intelligence Act in March 2024 (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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) (Text with EEA relevance) PE/24/2024/REV/1). The first solutions of the AI Act entered into force on 1 August 2024.

2 Since 2017, technologies such as the internet of things (IoT), artificial intelligence (AI), including avatars, as well as augmented and virtual reality (VR) have emerged and have been disseminated in the DigComp regulatory area. Also, such phenomena as cybercrime, disinformation, cyber security and the environmental aspects of the use of information technologies have emerged or increased in importance.

3 It is not the role of the Authors at this point to discuss the definition of artificial intelligence and its solutions from the technology and information perspective but, only in relation to its normative framework indicated by the European Union, to designate its place in the system of public policies.

Digital skills and knowledge of artificial intelligence among employees: results of the research

The normative framework of the DigComp guidelines indicated above presents a description of digital competencies and groups them into five areas: Information, Communication, Content Creation, Security and Problem Solving (starting from 2016, the areas include: Information and Data, Communication and Collaboration, Digital Content Creation, Security, Problem Solving and, starting from 2017, 8 skill levels). In the aforementioned EU policy, a digitally competent person must be fluent in these five areas, and not just be able to use digital technology functions (Foreword: DigComp). In its regulations, the AI Act, too, by dividing AI into four risk levels, also places certain restrictions on employers in relation to employees.

Hence, what is important in the research assumption is the presence not only in public policies (as indicated above on the example of EU policies), but also in the minds of citizens (both employers and employees). The bridge between digital policymaking and its practical applications consists in an effective use of emerging technologies and a translation of these technologies into feasible initiatives and policies also at the national level alongside EU regulations. By identifying key gaps and answering the research questions posed, we may provide a conceptual framework for the policy makers of these public policies. For this purpose, a pilot survey was carried out using the CAWI method[4]. The survey was categorized as a pilot survey because, with due argumentation of the selection of this tool, it showed its shortcomings in this case, giving a low response rate, one that did not allow the obtained research sample to be considered valid for the population. A decision was made to distribute the questionnaire to entrepreneurs through economic local governments, which possess geographical (territorial: regional) associations of entrepreneurs. The questionnaire was sent to forty chambers of commerce in Poland, with a request to distribute the research questionnaire among affiliated entrepreneurs. Unfortunately, only twenty-two entities responded.

4 The CAWI (Computer-Assisted Web Interviewing) research method is a survey data collection technique in which respondents answer questions via the internet by completing an online questionnaire. It is one of computer-assisted methods, along with CATI (Computer-Assisted Telephone Interviewing) and CAPI (Computer-Assisted Personal Interviewing).

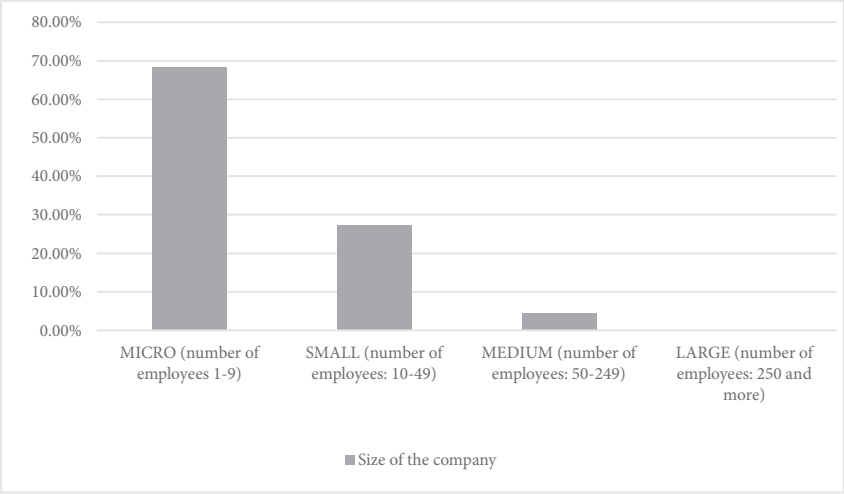
The aim of the pilot study is to better understand the needs of the labor market as regards the requirements of employers in the context of the development of new technologies. Their requirements over the next five years concerning the skills of employees in the ICT area (according to the DigComp skills grouping of categories) and the knowledge of the employers themselves on the public policies functioning in the area of artificial intelligence were examined.

The anonymous survey contained six substantive closed-ended questions, responses were collected in July 2024 (the holiday period may have been a negative factor for the survey sample size).

The characteristics of the respondents are as follows: according to the classification of *the Polish Classification of Activities* (*PKD*)[5], the highest percentage of responses came from representatives of the hotel and catering industry (27.3%); the manufacturing section and the financial advisory and insurance section account for 13.6% of the respondents. The micro-enterprise (with the following number of employees: 1–9) accounts for the highest response rate (68.2%). No responses could be obtained from representatives of macro enterprises.

5 *The Polish Classification of Activities* (*PKD*) is an economic classification system used to describe the type of activities carried out by companies and institutions in Poland. This is an equivalent of international classifications such as NACE in the European Union. PKD is used, among others, in statistics, public administration, accounting and legislation as a hierarchical classification divided into several levels. For the purposes of the survey, the respondents were asked to select one business option based on the sections of the PKD: A - Agriculture, forestry, hunting and fishing; B - Mining and quarrying; C - Processing industry; D – Production and supply of electricity, gas, steam and hot water; E - Water supply; sewage and waste management and remediation activities; F - Construction; G - Wholesale and retail trade; repair of motor vehicles including motorcycles H - Transportation and storage; I - Accommodation and catering services; J - Information and communication; K - Financial and insurance activities; L - Real estate activities; M - Professional, scientific and technical activities; N - Administrative and support service activities; O - Public administration and defense; compulsory social security; P - Education; Q - Health care and social assistance; R - Arts, entertainment and recreation activities; S - Other service activities; T - Activities of households as employers; production of goods and services for own use; U - Extraterritorial organizations and bodies.

Fig. 1: Share of respondents by size of enterprise



Source: Authors' own elaboration based on data collected.

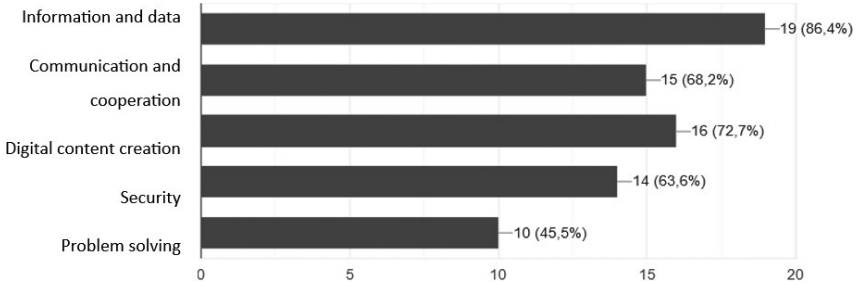
When asked which areas (according to the areas indicated in DigCamp)[6] the entrepreneurs think will be important in their company in the next five years and at the same time expected from their employees, the area: 'Information and data' was indicated first (multiple answers could be indicated). The least important areas for employers included issues related to technical problem

6 The areas identified in DigCamp are as follows: 1. 'Information and Data' (a - Browsing, searching and filtering data, information and digital content; b – Evaluation of data, information and digital content; c – Management of data, information and digital content); 2. 'Communication and Collaboration' (a - Communicating using digital technologies; b - Sharing information and resources using digital technologies; c - Active citizenship using digital technologies; d - Collaborating using digital technologies; e - Netiquette; f - Managing digital identity); 3. 'Creation of digital content' (a – Creation of digital content; b - Integrating and processing digital content; c - Complying with copyright and licensing; d - Programming); 4. "Security" (a - Tools for protection; b - Protecting personal data and privacy; c - Protecting health and well-being; d – Environmental protection); 5. "Problem solving" (a - Solving technical problems; b - Identifying technological needs and solutions; c - Creative use of digital technologies; d - Identifying digital competence gaps).

solving, recognition of technological needs and solutions, creative use of digital technologies or recognition of digital competence gaps (competence group: 'Problem solving').

The model presented above is confirmed by the next question, where entrepreneurs also indicated the area of "Problem solving" as the least expected among the skills to be possessed by employees in the next five years. Significantly, this area includes not only technical issues but also recognition of digital competence gaps. However, this question would require deeper analysis due to the survey tool used. Definitely standing out among the digital competencies desired by employers in the near future were two areas, being in fact quite independent of the declared industry of the entrepreneur. These areas included: 'Information and Data' (which includes: browsing, searching and filtering data, information and digital content; evaluation of data, information and digital content; managing data, information and digital content) and 'Digital Content Creation' (which includes skills such as: creating digital content; integrating and processing digital content; complying with copyright and licensing; programming).

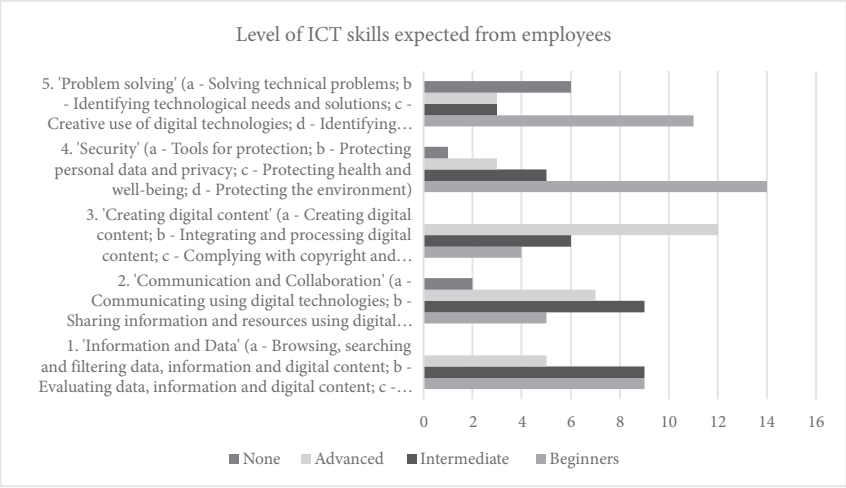
Fig. 2: Areas that entrepreneurs believe will be important in their company in the next five years and at the same time expected by them from their employees



Source: Authors' own elaboration based on data collected.

Production of digital content is also an area whose skill level more than half of employers would see in their employees at an advanced level. While the issue of security (including security tools, data protection and privacy, healthcare and well-being or environmental protection) is declared as a desirable skill by almost three-quarters of the respondents at an entry level, the issue of problem solving (probably interpreted at the technical level by the respondents) was among the skills indicated as not required for recruitment.

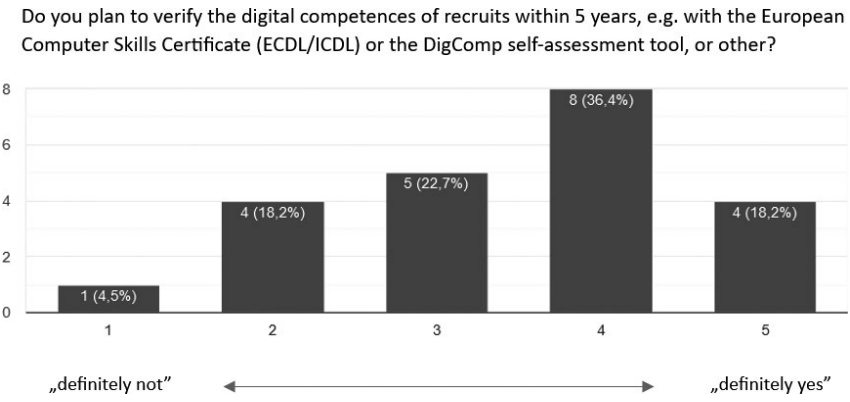
Fig. 3: Level of ICT skills expected by employers in employees over the next five years



Source: Authors' own elaboration based on data collected.

Responding on the Likert scale ranging from "definitely not" to "definitely yes" to a question concerning the desire to verify digital skills among employees in the next five years, more than half of the respondents expressed a desire for such verification.

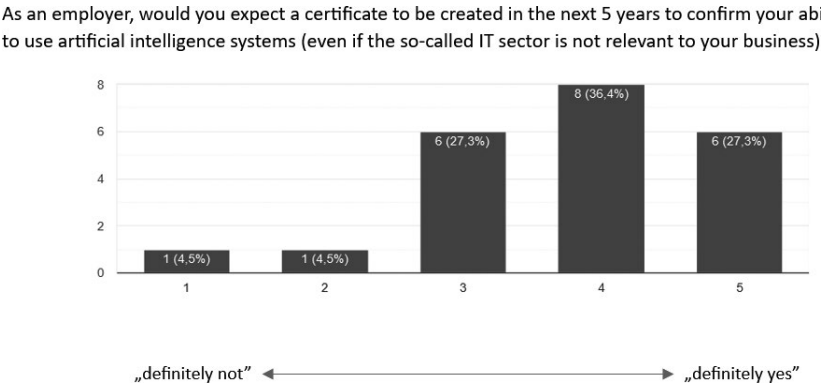
Fig. 4: Declaration of verification of ICT skills among employees in the next five years by employers



Source: Authors' own elaboration based on data collected.

The need for raising AI issues and, in particular, its certification as part of not individual but systemic solutions among public policies was indicated by entrepreneurs in the next question. Asked whether they would expect in the next five years to create a certificate confirming an ability to use artificial intelligence systems (even if the so-called AI sector is not relevant to your business), more than 63% of the respondents answered in the affirmative (answering on the Likert scale).

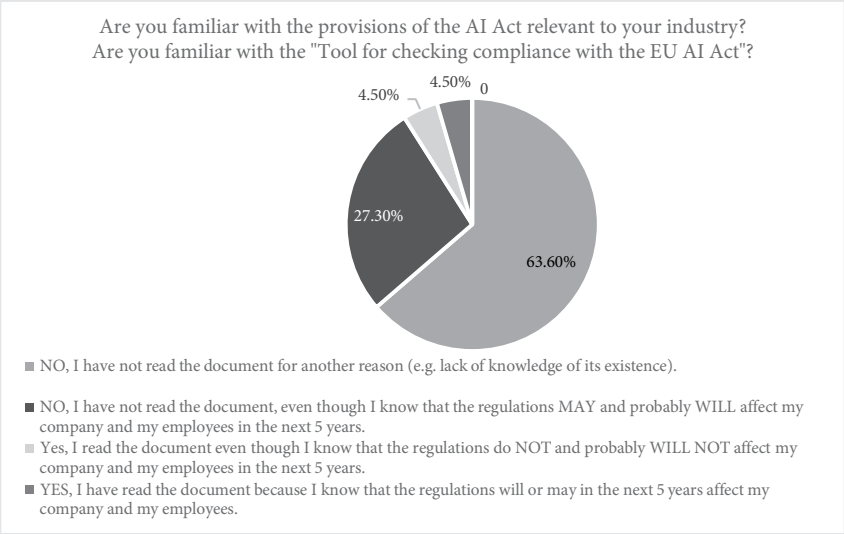
Fig. 5: Level of expectation by employers in the next five years to create a certificate to prove ability to use artificial intelligence systems



Source: Authors' own elaboration based on data collected.

In July 2024, the Artificial Intelligence Regulation (AI Act) was published in the Official Journal of the European Commission. The AI Act aims to ensure safe and ethical use of artificial intelligence technology. The new regulations include requirements for the transparency of algorithms, labeling of AI-generated content or lifecycle management of AI systems, introducing AI risk levels, among other things. The regulations introduce new obligations for entities located in and outside the EU. When surveyed on whether the respondents were familiar with the provisions of the AI Act pertaining to their industry along with a tool to assist businesses in verifying compliance with the EU AI Act, they indicated a definite (more than 90%!) lack of familiarity with the aforementioned regulations. This was mostly due to a lack of knowledge of how the AI Act functions in the normative system, although there were also responses confirming unfamiliarity with the regulation despite an awareness that it may apply to employers themselves.

Fig. 6: Businesses' familiarity with the provisions of the AI Act and the 'Tools for checking compliance with the EU Artificial Intelligence Act'



Source: Authors' own elaboration based on data collected.

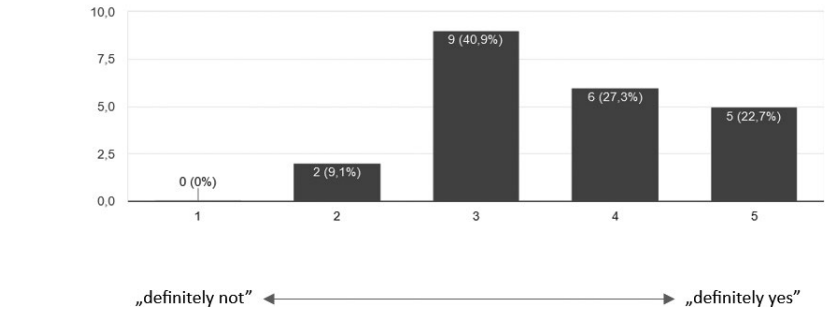
The last question addressed the concerns of entrepreneurs in relation to the prevalence of generative artificial intelligence (e.g., Chat GPT, BERT, BING) in everyday life causing a reduction in critical thinking skills among employees. Although 40.9% of the entrepreneurs, answering again on the Likert scale, takes a neutral approach to this question, a total of almost 50% have or even definitely have such concerns.

The responses presented above show the state of knowledge on normative regulations on AI by businesses, the need to implement into public policies not only knowledge of AI but also universal certification of ICT skills. It was indicated what skills and at what level will be desired by employers in the economic sector among employees over the next five years, and the pilot results may indicate a trend that requires in-depth research.

Summary

This study offered a partial answer to the research questions posed. On the one hand, entrepreneurs declare that employees in the next five years will possess skills in the areas of digital competencies, particularly data retrieval and digital

Fig. 7: Businesses' concerns about causing a reduction in critical thinking skills among employees through the prevalence of generative artificial intelligence (e.g. Chat GPT, BERT, BING) in everyday life



Source: Authors' own elaboration based on data collected.

content creation. They are also interested in verifying the skills referred to and taking into account unification within public policies of the validation of artificial intelligence skills. Thus, it seems that given employers' concerns that are not so substantial about the reduction through the prevalence of AI of employees' logical thinking abilities, the use of AI may become a desirable skill among employers. Is the scenario of AI not 'taking away' jobs but transforming them possible? This is a question that requires in-depth and further research. A strong recommendation is proposed to introduce a broader process of information about the EU solutions to the AI Act into public policies, as more than 90% of the respondents are not aware of the aforementioned provisions and almost half express concern about a reduction of critical thinking skills among employees by the development and availability of new technologies. When answering the research questions (RQ1 and RQ2), the following was therefore indicated:

a) Those elements that require implementation in public policies include: information among entrepreneurs regarding the AI Act and an EU tool to support self-qualification of AI risk levels. This is due to the low state of knowledge among entrepreneurs regarding AI public policies;
b) Entrepreneurs' expectations for the validation of AI skills among employees as an element of ICT, required at a minimum basic level in most ICT areas (according to the classification of ICT areas by DigComp) in the next five years;

c) Expectations and concerns on the part of business sector entrepreneurs related to the workforce and the development of new technologies over the next five years, indicating primary interest (according to the classification of ICT areas by DigComp) in data acquisition and digital content creation.

Considering the small percentage of the responses obtained, the part based on the economic sector's own survey should be regarded only as a pilot study, however, one that is indicating a certain trend. Future in-depth studies should take into account the potential of more case studies for the correct drawing of conclusions and their transfer for the purpose of the creation of state public policies.

The development of employee competencies brings many benefits both to employees and organizations. Employees with the right competencies are more productive in their jobs. Developing skills related to their positions or industry may increase the productivity and efficiency of their work. With the right digital skills in place, employees can be more engaged, open to new growth opportunities, operating costs may be reduced and a strong employer brand may be built.

The current labor market makes digital competencies mandatory for any person who wants to work professionally. Drawing any maps of the space of digital human activity is always a cause of dissatisfaction. This is due to the various possibilities of approaches to the problem on the one hand and the multifaceted nature of capturing the most important fragments of man's being in time and space that characterize their being on the other.

Every organization needs a strategy to continuously improve the digital competencies of its employees. As it can be observed, the practice of retraining new employees in terms of these competencies is rarely used by employers. The preferred strategy is to hire new employees with the right skills that immediately meet the needs of the company, yet this is not the case in reality. Hence, companies should support an acquisition of digital competencies by employees. At the same time, as recent research indicates, the importance of strategic support in digital transformation policies, where the (emerging) digital technology serves not only as an infrastructure to support public administration but also as a catalyst for progress, is relevant at the level not just of an individual entrepreneur but of comprehensive public policies (Lee, Kim and Yoon 2024).

References

Bauman, Zygmunt, *Płynny lęk* (Kraków: Wydawnictwo Literackie, 2008).

'Biała Księga w Sprawie Sztucznej Inteligencji Europejskie Podejście Do Doskonałości i Zaufania White Paper on Artificial Intelligence: A European

Approach to Excellence and Trust English COM(2020)/' (2020) <https://commission.europa.eu/document/d2ec4039-c5be-423a-81ef-b9e44e79825b_pl> accessed 21 June 2024.

Beck, Urlich, *Społeczeństwo ryzyka: w drodze do innej nowoczesności* (Warszawa: Wydawnictwo Scholar, 2004).

Berkeley, Holly, *Marketing internetowy w małej firmie* (Gliwice: Wydawnictwo Onepress, 2005).

Buczyńska-Łaba, Justyna, Krasińska, Barbara, 'Projekt Digital Humanities Labolatory Info Uniwersytetu Pedagogicznego w Krakowie jako przykład przedsięwzięcia prowadzącego do technicyzacji pracy w bibliotekach naukowych oraz próba wykorzystania humanistyki cyfrowej w nauczaniu akademickim', in: Joanna Czyrek, Bożena Górna, ed., *Nowe projekty, cenne inicjatywy i ciekawe przedsięwzięcia bibliotek naukowych* (Wrocław: Wydawnictwo Korporacja Bibliotekarzy Wrocławskich, 2016), 24–36.

Carretero, Stephanie, Vuorikari, Riina Hannuli, Punie, Yves, Urban, Katarzyna, and Ministerstwo Cyfryzacji, ed., *DigComp 2.1: ramy kompetencji cyfrowych dla obywateli z ośmioma poziomami zaawansowania i przykładami zastosowania* (Lublin, Ministerstwo Cyfryzacji, 2017).

Chałubińska-Jentkiewicz, Katarzyna, and Karpiuk, Mirosław, *Prawo Nowych Technologii: Wybrane Zagadnienia* (Warszawa, Wydawnictwo Lex, 2015).

'Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 Establishing the Digital Decade Policy Programme 2030 (Text with EEA Relevance), PE/50/2022/REV/1' <https://eur-lex.europa.eu/eli/dec/2022/2481/oj> accessed 21 June 2024.

European Parliament, 'Digital Agenda for Europe: Fact Sheets on the European Union', 2024 <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe> accessed 21 June 2024.

Fenlon, Katrina, Frazier, Emily, and Muñoz, Trevor, 'Digital Humanities', *Reference Module in Social Sciences* (2024), 2–10.

Harari, Juwal, Noach, *21 lekcji na XXI wiek* (Warszawa: Wydawnictwo Literackie, 2018).

Hyytinen, Heidi, Toom, Auli, and Postareff, Liisa, 'Unraveling the Complex Relationship in Critical Thinking, Approaches to Learning and Self-Efficacy Beliefs among First-Year Educational Science Students', *Learning and Individual Differences* 67 (2018), 132–42.

Juraszek, Dawid, *Antropocen dla początkujących. Klimat, środowisko, pandemie w epoce człowieka* (Łódź: Wydawnictwo Fundacji Liberte, 2020).

Kaczmarek, Krzysztof, Karpiuk, Mirosław, Melchior, Claudio, and, 'A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data', *PRAWO i WIĘŹ* 50/3 (2024), 103–121.

Kołodziejczyk, Adam, 'Bezpieczeństwo. Kontekst personalno-aksjologiczny', *Nauki o Zarządzaniu Zeszyty Naukowe WSOWLąd*. 1/151 (2009), 140–152.

Kuliczkowski, Marian, *Pozamilitarne przygotowania obronne w Polsce. Próba systematyzacji procesualnych oraz funkcjonalnych aspektów przygotowań* (Warszawa: Wydawnictwo AON, 2016).

Lee, Joong-Yeup, Kim, Beomsoo, and Yoon, Sang-Hyeak, 'A Conceptual Digital Policy Framework via Mixed-Methods Approach: Navigating Public Value for Value-Driven Digital Transformation', *Government Information Quarterly* 41/3 (2024), 10196.

Łomny, Zbigniew, *Człowiek i edukacja wobec przemian globalnych* (Radom: Wydawnictwo Instytutu Technologii Eksploatacji, 1996).

Manovich, Lev, *Język nowych mediów* (Warszawa: Wydawnictwo Akademickie i Profesjonalne, 2006).

Morbitzer, Jerzy, *Edukacja wspierana komputerowo a humanistyczne wartości pedagogiki* (Kraków: Wydawnictwo Naukowe Akademii Pedagogicznej, 2007).

Newman, David, Webb, Brian R., and Cochrane, Clive, 'A Content Analysis Method to Measure Critical Thinking in Face-to-Face and Computer Supported Group Learning', *Interpersonal Computing and Technology Journal* 3 (1995), 56–77.

Pieczywok, Andrzej, 'Edukacyjne wyzwania bezpieczeństwa człowieka', in Małgorzata Czuryk, Krzysztof Drabik, Andrzej Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych* (Olsztyn: Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego, 2018), 180–270.

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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) (Text with EEA Relevance) PE/24/2024/REV/1' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689> accessed 21 June 2024.

'Słowo wstępne – DigComp' <https://www.digcomp.pl/slowo-wstepne/> accessed 21 June 2024.

Suchodolski, Bogdan, Wojnar, Irena, *Humanizm i edukacja humanistyczna* (Warszawa: Wydawnictwo WSiP, 1988).

Toffler, Alvin, *Trzecia fala* (Warszawa: Państwowy Instytut Wydawniczy, 1985).

'Treaty on the Functioning of the European Union of 13 December 2007 — Consolidated Version (OJ C 202, 7.6.2016)' <https://eur-lex.europa.eu/EN/

legal-content/summary/treaty-on-the-functioning-of-the-european-union.html> accessed 21 June 2024.

Wechsler, Solange Muglia, Saiz, Carlos, Rivas, Silvia F., Vendramini, Claudete Maria Medeiros, Almeida, Leandro S., Mundim, Maria Celia, et al., 'Creative and Critical Thinking: Independent or Overlapping Components?', *Thinking Skills and Creativity* (2018), 114–22.

Witecka Małgorzata, 'Cyberterroryzm', in Maciej Marszałek, ed., *Zwalczanie terroryzmu* (Warszawa: Wydawnictwo AON, 2014).

Włodyka, Ewa, 'Gotowi – Do Startu – Start? Przyczynek Do Dyskusji Nad Gotowością Jednostek Samorządu Terytorialnego Do Zapewniania Cyberbezpieczeństwa', *Cybersecurity and Law* 7/1 (2022), 202–19.

Wojnar, Irena, 'Światowa dekada rozwoju kulturalnego – nowe propozycje dla edukacji', in Irena Wojnar, Jerzy Kubin, ed., *Edukacja wobec wyzwań XXI wieku* (Warszawa: Dom Wydawniczy, 1996), 25–35.

Agnieszka Łukasik-Turecka*, Martinas Malužinas**

Strategies to Counter Russian Disinformation: Case Study of Lithuania

Abstract: The aim of the chapter is to present strategies of counteracting Russian disinformation on the example of Lithuania. It is to be realised by analysing the content of disinformation messages present in the Lithuanian information space, dedicated to the Russian aggression on Ukraine and disseminated mainly by new media, but first of all, by analysing actions taken by Lithuanian authorities in order to limit the influence of Russian media and increase the level of public awareness of information threats and increase resistance to disinformation.

Keywords: disinformation, counteraction, media education, war in Ukraine, Lithuania, Russia

1. Introduction

Disinformation has long been well-established in Russian foreign policy (Nehring, 2017). Although still based on Cold War tactics, contemporary disinformation conducted by the Russian Federation presents unique characteristics. As Francesco Bechis points out: 'This is not just due to the use of social media and new technologies, but also because it has changed scope, speed, and volume. Today Russian disinformation campaigns can count on a wholly new set of tools. Social media platforms and the pro-government media environment provide them with a much higher level of discretion than the Soviet ones, making it more difficult to trace them back to government agencies' (2020: 122).

The annexation of Crimea and Russia's full-scale invasion of Ukraine opened a new chapter of Russian propaganda and disinformation directed against NATO countries (Kaczmarek, Karpiuk, Melchior, 2024: 110). The Russian Federation's aim from the outset was to remove responsibility from the Kremlin for the war in Ukraine, blaming Ukraine, the US and NATO for the invasion (Musiał-Karg & Lukasik-Turecka, 2023). Russia has a particular claim to the states created on the basis of the former Soviet republics. In relation to states such as Lithuania,

* *The John Paul Catholic University of Lublin, ORCID ID: 0000-0003-3657-9862, e-mail: agnieszka.lukasik-turecka@kul.pl*

** *Koszalin University of Technology, https://orcid.org/0000-0002-2772-9534, e-mail: martinasmaluzinas@gmail.com*

Russia has strategic objectives, including: influencing solidarity within NATO and the European Union, reproducing the Russian narrative, spreading false information, provoking extreme social and political attitudes, and demonstrating the incompetence of the Lithuanian government or the country's insolvency (Fraszka, 2020: 2–16).

This chapter aims to present the strategy of countering Russian disinformation using Lithuania as an example. In order to examine and evaluate the actions taken in Lithuania aimed at countering Russian disinformation, before starting the research, an initial thesis was adopted stating that the main factor influencing the occurrence of false and intentional information in the Lithuanian media space is the information warfare conducted by the Russian Federation, which also covers the media space of Lithuania. The main research question concerned the tools used to counter Russian disinformation in Lithuania and whether they provide effective protection against the harmful influence of false information. In order to achieve the research goal, the case study method was chosen, which involves a closer look at a specific case and drawing conclusions about the causes, direction and chosen strategy of actions, in this case Lithuania, in the fight against disinformation. The research material consisted of expert reports, which allowed to determine the positions, attitudes and strategies implemented by Lithuanian decision-makers.

2. Defining disinformation and ways to counter it

There is no single, universally accepted definition of disinformation. The difficulty in defining the phenomenon of disinformation is due to a number of reasons. First of all, from the multiplicity of terms that are close or even identical, such as distorted communication, propaganda or clickbait, from the large number of definitions of the term 'disinformation' itself, varied due to different research approaches (Kupiecki, Bryjka, Chłoń, 2022: 64–66; Bakowicz, 2023: 94, 106), and also because the phenomenon of disinformation is described using broad, not always correctly defined terms that do not comply with international legal standards (Human Rights Council, 2021). When defining the term 'disinformation', the emphasis is usually on the simultaneous presence of two elements: false information and intentionality of actions, thus distinguishing disinformation from misinformation and malicious information (See more extensively Wardle, Derakhshan, 2017; NATO, 2020; European Commission, 2022).

Various typologies of disinformation can be found in the literature. One of the more interesting ones is the typology of disinformation, which takes into account the criteria of purpose, the importance of the objectives that disinformation supports, and the complexity of the mechanisms that serve this purpose. Based on

these criteria, we divide disinformation into: ad hoc and simple, or tactical - used in the simplest of situations; complex, or operational - used in longer or repetitive time sequences, concerning multi-threaded issues; and strategic, used to achieve long-term goals (Kupiecki, Bryjka, Chłoń, 2022: 65).

The difficulty in clearly defining disinformation translates into choosing appropriate responses to it and finding ways to counter it (Human Rights Council, 2021). Nevertheless, the presence of disinformation in the information space prompts questions about the possibilities of countering it, due to the fact that in the age of the internet and huge technological changes, it is becoming a weapon in the hands of states and other actors on the international political scene, causing great damage. As Robert Kupiecki, Filip Bryjka and Tomasz Chłoń emphasise, traditional knowledge of an adversary's aims and methods and knowledge of the codes of intelligence, diplomatic and political culture are not enough to fight disinformation today. In order to fight disinformation, a holistic and integrated approach is needed, combining and mobilising both state structures or inter-ministerial teams, as well as civil society, civil society organisations, academics, journalists and ordinary internet users. The idea is to combine these resources into a national as well as an international counteraction. An example of such spontaneous action on a global level was the reaction of the international community to Russia's invasion of Ukraine, which consisted of informing the Russians about real events on the frontline via text messages, e-mails or phone calls by whole crowds of ordinary internet users. Another example was a grassroots hacking campaign to block the websites of Russian institutions and their channels disseminating propaganda messages (2022: 192–193).

A major role in countering disinformation is attributed to media education (Salomaa, 2024; Kupiecki, Bryjka, Chłoń, 2022: 193). While effective methods of combating disinformation are expected from state services and experts, the effect of combating disinformation depends just as much on the attitudes of individual media users. These attitudes, in turn, result from acquired knowledge, awareness of the threat and the development of critical media literacy skills, which are most easily acquired through media education and, more broadly, public education (Kupiecki, Bryjka, Chłoń, 2022: 193). A good example is the approach of Finland, where media literacy has for years been included in the Security Strategy for the Society and treated as part of psychological resilience of the society (as part of psychological resilience). This approach is based on the idea that the most important functions of society are carried out jointly, through the cooperation of authorities, business, organisations and citizens, and that a secure, also in the context of disinformation, and crisis-resilient Finland is built together, not relying only on the actions of the security authorities (Salomaa, 2024).

Countering disinformation can be considered at three levels: the individual, corporate and civil society, and at the state and international levels. At the level of the individual, being equipped with basic psychological knowledge and social competence, one can relatively quickly develop the necessary habits of verifying information and not giving in to easy instincts. As Robert Kupiecki, Filip Bryjka and Tomasz Chłoń emphasise, we will not completely eliminate disinformation from interpersonal communication, as it is in a sense a natural phenomenon, and demographic factors, age, sources, celebrities, increased mental activity, personal traits, propensity for analysis, emotionality or morality also contribute to its spread. At the individual level, it is important to take care of behavioural hygiene in the information space, which includes checking the credibility of sources, the author of the publication and his/her previous publications, the date of publication, or verifying information in other sources (2022: 216–217).

At the corporate and civil society level, there is much to be desired in the actions of social media platform owners. In the face of public pressure, proactive actions by platforms can include protecting children and young people from disinformation and aggression, addressing health issues and combating extremism, as well as responding more proactively to political manipulation and extremism and limiting opportunities to make money from disinformation. However, the researchers emphasise that without thoughtful regulatory coercion by major states and international organisations, the social media situation in the area of countering disinformation will not fundamentally change. According to the researchers, the most important role in combating disinformation is played by civil society, in particular the research, education and media communities. It is they who help to identify disinformation, provide expertise, educate both service representatives and ordinary media users (Kupiecki, Bryjka, Chłoń, 2022: 222–247).

At the state level, Kupiecki, Bryjka and Chłoń included among the activities aimed at countering disinformation: the creation of structures to combat foreign disinformation, the creation of legal regulations, the adoption or amendment of national cyber security strategies, education of authorities and officials, warnings to authorities, administrative decisions concerning, for example, the withdrawal of a licence from a given medium, diplomatic actions and cooperation with the public. It is also crucial to counter disinformation from a regional perspective, but also at the international level, within the European Union, NATO and the UN. As the researchers point out, a coherent Western response and the building of societal resilience to disinformation, both at the national and international level, should focus on strengthening this resilience, expanding offensive prevention activities, bridging differences in the practical approach to disinformation among Western states (2022: 248–277).

3. Disinformation in the Lithuanian information space and its counteraction

The information warfare waged by the Russian Federation in Lithuania's information space is mainly implemented through the creation and dissemination of numerous disinformation messages. These activities intensified after the start of Russia's full-scale war in Ukraine.

In 2023, the Lithuanian armed forces recorded 3520 unique cases of hostile information activity, of which 2148 were directly related to state security (kam.lt, 2023: 21). For example, in May 2023, Lithuanian military experts identified 95 specific cases of defence-related disinformation in Lithuania's hostile information environment. The three main themes of disinformation concern the war in Ukraine, Lithuania's membership in NATO and the relationship between NATO and Russia. The aim of the misinformation was to convince the Lithuanian public that Lithuania's support for Ukraine was leading to an escalation of the conflict, and that NATO was the aggressor and Russia and Belarus needed to defend themselves against the Alliance states (wilno.tvp.pl, 2023a).

In order to counter the Kremlin's disinformation activities, Lithuanian political elites have taken a number of measures to detect and combat disinformation, at various levels of countering it. One of the important measures in this direction at the state level was the creation of a model for the management of Lithuania's cyber security system as early as 2014, the specificity of which is regular and intensive cooperation between state institutions, uniformed services and institutions and entities classified as so-called critical infrastructure (such as energy companies, financial institutions or health care, among others). This also resulted in the creation of the National Cyber Security Centre (NCC) in 2015 and the reform of the Cyber Security Law in 2017, which provides for the central management of the security of information resources and the comprehensive integration of the monitoring of Lithuania's electronic communication networks. In 2019, the law was amended to allow authorised institutions of the Lithuanian state (including the NCC) to block servers for a short period of time to entities that are used to spread fake news (Dudzinska, 2019: 1).

Another solution to counter Russian online trolls and bots was the establishment of the so-called elf movement in 2017. This is an example of counteraction at the civil society level. This movement, mainly made up of Lithuanian volunteers, focuses on identifying, unmasking and combating Russian disinformation in the online space by detecting fake accounts. Within the framework of the aforementioned movement, the Demaskuok.lt platform has also been created, bringing together representatives of state institutions, but also journalists and IT specialists

to deepen cooperation and coordination in the fight against false information (UKEN, 2020). The platform's concept relies heavily on artificial intelligence to analyse more than 30,000 articles per day, written in Lithuanian and Russian, and from 2020 also those developed in Latvian and Estonian. Expanding the scope of its impact, the Demaskuok.lt platform is attracting the attention and source of funding from global companies such as, among others: Google, as well as media giants such as The Financial Times and Deutsche Welle. A tangible result of Demaskuok.lt's collaboration with Google was the creation of the Digital News Innovation Fund. The Lithuanian organisation presented its operations and principles in 17 countries, including the US, Germany, the UK, France, Serbia and other regions of the world (delfi.lt, 2020). As a result of the intensive work of the elf movement, an online database Vatnikas.lt was created in 2017, in which the names of Russian trolls are regularly revealed (Vasiuta, Vasiuta, 2020, 136–147). Since 2018, Demaskuok.lt has been actively cooperating with the Strategic Communications Department of the Lithuanian Armed Forces (STRATCOM), the Office of Threat Management and Crisis Prevention of the Chancellery of the Government of the Republic of Lithuania, the Lithuanian Rifle Association and the public institution 'Res Publica' (Lietuvos šaulių sąjunga, 2018).

In addition, a success of the Lithuanian state in the fight against disinformation is the creation of a military platform; its activity demonstrates the commitment of military structures in the fight against disinformation. It constantly monitors what information is spread by the media and where it comes from (Konieczny, 2022: 23).

In addition, since 2015, the National Cyber Security Centre (NCSC) was established under the Ministry of Defence, which is the main cyber security institution in Lithuania, responsible for the cyber security of critical information infrastructure and the accreditation of information and disinformation resources (nksc.lt, 2023).

It is noteworthy that since the annexation of Crimea by Russia, the Lithuanian government has made efforts to limit the influence of Russian media in its public sphere, which are funded by Russian government sources (Lietuvos Respublikos valstybės saugumo departamentas, 2014). In turn, in 2019, the Lithuanian Seimas voted to amend legislation that allows the Lithuanian Television and Radio Broadcasting Commission (LRTK) to immediately cease broadcasting TV channels in a situation of state security threat. In 2022, following the full-scale aggression of the Russian Federation against Ukraine, the Lithuanian Parliament passed a law banning the broadcasting of Russian as well as Belarusian TV channels (Lrt.lt, 2022).

Moreover, internationally, Lithuanian political elites were one of the most active initiators of sanctions on Russian propaganda TV channels, which were imposed

by the European Union in 2022. Among the Russian media whose programmes were broadcast to Lithuania, the EU sanctions included Russian government news agencies like Sputnik and its affiliates: Sputnik Arabic, Russia Today and its subsidiaries, including Russia Today English, Russia Today UK, Russia Today Germany, Russia Today France, Russia Today Spanish, Russia Today Arabic, Rossija RTR / RTR Planieta, Rossija 24/Russia 24, Rossija 1, TV Centre International, NTW/ NTV Mir, REN TW, Pervy Kanal, Oriental Review, Tsargrad TV Channel, New Eastern Outlook, Katehon,Kanal Spas, Voice of Europe, RIA Novosti, Izvestia, Rossiyskaya gazeta (Kaca, 2024).

Lithuania's strategy to reduce the influence of Russian media is based on creating an open, clear, democratic and independent information environment that is also accessible to Russian and Polish speakers, especially those living in the Vilnius region. The Lithuanian authorities' efforts to improve information security in the country consist of building an increased level of awareness of information threats among citizens, as well as shaping resistance to manipulation (Kuczyńska-Zonik, 2022).

There is also a social and political consensus in Lithuania that more resources should be allocated to control the spread of disinformation. A survey conducted by Spinter Research for the European Commission Representation in Lithuania showed that the majority of Lithuanians (88%) believe that more resources should be allocated to control the spread of disinformation in Lithuania (15min.lt, 2024). In 2023, representatives of all clubs and circles in the Seimas, together with the Lithuanian Prime Minister, in view of Russia's active efforts to undermine democratic processes in Lithuania through disinformation, decided to register amendments to the Criminal Code and the Law on Public Disinformation. If adopted, the amendments would entail criminalising online manipulation, where content directed against the Lithuanian state is artificially amplified and promoted. This would be punishable by penalties ranging from a fine or arrest to imprisonment of up to 3 years. Individuals (Lithuanian citizens) and entities (including companies and organisations of different nature and activities in different fields) would be held liable (wilno.tvp.pl, 2023b).

One of the effective tools under the Lithuanian authorities' counterdisinformation strategy remains active and regularly organised inter-institutional public counterdisinformation campaigns. Their specificity lies in the development of a governmental capacity to coordinate strategic communication, which is managed and controlled by individual Lithuanian ministries and departments (e.g. by the National Security Commission), with parliamentary control in the committees of the Seimas, which brings together and coordinates the cooperation of state institutions, with NGOs (e.g. Debunk.eu) and academia (Vilnius University Institute of

International Relations and Political Science- VU TSPMI, Eastern Europe Studies Centre - RESC). The overarching goal of the analysed strategy is to strengthen the resilience of Lithuanian society (Eastern Europe Studies Centre, 2020: 4).

In addition, Lithuania's inter-institutional strategy on disinformation campaigns actively seeks to deepen cooperation with international organisations. In 2024, Lithuania and the OECD developed an international programme to counter disinformation. Lithuanian state institutions, in cooperation with the Organisation for Economic Co-operation and Development (OECD) and partner governments and other sectors, will exchange knowledge and experience in identifying disinformation and choosing the most effective ways and means to stop its spread. Following the signing of the agreement, the National Crisis Management Centre, is designated as the implementing agency of the programme on the Lithuanian side, tasked with ensuring the management of activities, mobilising expertise and organising training and seminars. On the other hand, it remains the responsibility of the OECD to identify a potential training area, to offer experts from OECD and non-OECD countries the opportunity to enhance their knowledge and competencies under the programme (Lrt.lt, 2024).

4. Conclusions

The annexation of Crimea and the full-scale invasion of Ukraine by the Russian Federation has opened a new chapter in the history of Russian disinformation. New technologies, the internet and social media are causing pro-Kremlin disinformation messages to reach larger and larger masses of audiences and at ever-increasing speed.

The primary factor influencing the occurrence of false and intentional information in the Lithuanian media space is the information war waged by the Russian Federation, which also extends to the Lithuanian media space. Lithuania uses all possible tools to counter Russian disinformation. As part of its strategy to counter Russian disinformation, Lithuania has been taking a number of measures since 2014. Many of them are taken at the highest - state and international - level, such as the governance model of Lithuania's cyber security system, which was already created in 2014, or the National Cyber Security Centre, established in 2015. Another important step was the reform of the Cyber Security Law in 2017 and the amendment of the law in 2019, allowing authorised institutions of the Lithuanian state to block servers for a short period of time to entities that are used to spread fake news.

Equally important activities are undertaken at the level of civil society. An example is the elf movement described above, which brings together mainly Lithuanian volunteers to identify, expose and combat disinformation messages.

Reducing the influence of Russian media is also an extremely important activity; cooperation with international organisations is a good direction in this area. This is an example of countering disinformation at the international level.

The tools used by Lithuania to counter disinformation limit it, but do not provide total protection against false information. Certainly, a factor that makes countering disinformation messages difficult is the lack of a clear definition of disinformation, adopted by Lithuanian authorities. Difficulties in clearly defining disinformation translate into choosing appropriate responses to it and finding ways to counter it. However, this is a problem not only for Lithuania, but also for many other countries, so international cooperation is extremely important in the fight against disinformation.

References

Bąkowicz, Katarzyna, Narzędzia dezinformacji i manipulacji w przestrzeni medialnej i społecznej. Rodzaje, charakterystyka, oddziaływanie, In: B. Sosińska-Kalata, P. Tafiłowski (eds.) *Nauka o informacji w okresie zmian. Nauka wobec współczesności: wojny informacyjne*, Wydawnictwo Naukowe i Edukacyjne Stowarzyszenia Bibliotekarzy Polskich, Warszawa, (2023), 93–109.

Bechis, Florencia, Playing the Russian Disinformation Game. Information operations from Soviet tactics to Putin's sharp power, In: S. Giusti, E. Piras (eds.) *Democracy and Fake News. Information Manipulation and Post-Truth Politics*. Routledge, London, 2020, https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003037385-12/playing-russian-disinformation-game-francesco-bechis?context=ubx, retrieved: 01 August 2024.

delfi.lt, „Demaskuok.lt" žengia į Latvijos ir Estijos dezinformacijos lauką, https://www.delfi.lt/m360/naujausi-straipsniai/demaskuoklt-zengia-i-latvijos-ir-estijos-dezinformacijos-lauka-84246847?fbclid=IwY2xjawEZZrFleHRuA2FlbQIxMAABHeGlWUTQycdmvziqYzXSlFGFX5h1zbcVkDBRBwQCTl96XMb3dSEJefzS4g_aem_HyJRZLE6gkCc0W1GFiDAZw, retrieved: 11 May 2020.

Dudzińska, Kinga, Polityka Litwy na rzecz walki z dezinformacją, *Polski Instytut Spraw Publicznych* 67 (2019), https://pism.pl/publikacje/Polityka_Litwy_na_rzecz_walki_z_dezinformacj_, retrieved: 11 May 2020.

European Commission, 2022 Strengthened Code of Practice on Disinformation, 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, retrieved: 24 July 2024.

Eastern Europe Studies Center, LIETUVOS VISUOMENĖS KOVA SU DEZINFORMACIJA: SITUACIJOS ANALIZĖ IR REKOMENDACIJOS, 2020, https://www.eesc.lt/wp-content/uploads/2021/01/Lietuvos-visuomenės-

kova-su-dezinformacija-situacijos-analizė-ir-rekomendacijos.pdf, retrieved: 10 December 2022.

Fraszka, Bartosz, Państwo bałtyckie a rosyjskie zagrożenie, *Warszawa Instytut Raport specjalny* (2020), 2–16, https://www.google.com//warsawinstitute.org/pl/panstwa-bałtycki-rosyjski-zagrożenie-hybrydowe/, retrieved: 09 August 2024.

Human Rights Council, Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, 2021, https://documents.un.org/doc/undoc/gen/g21/085/64/pdf/g2108564.pdf?token=2rmVNaMrhwrBrgQWyU&fe=true, retrieved: 24 July 2024.

Kaca, Elżbieta, Znaczenie sankcji UE w przeciwdziałaniu rosyjskiej dezinformacji, *Polski Instytut Spraw Publicznych* 78 (2024), https://pism.pl/publikacje/znaczenie-sankcji-ue-w-przeciwdzialaniu-rosyjskiej-dezinformacji, retrieved: 24 July 2024.

Kaczmarek, Krzysztof, Karpiuk, Mirosław, Melchior, Claudio, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź", 4 (2024), 103–121, DOI: 10.36128/PRIW.VI50.907.

kam.lt, Leidinys 'Krašto apsaugos sistema', *Skaičiai ir pokyčiai* 2023, https://kam.lt/wp-content/uploads/2024/04/skaiciai-ir-pokyciai2023.pdf, retrieved: 04 August 2024.

Konieczny, Marcin, DEMASKUOK – THE LITHUANIAN SYSTEM TO COUNTER DISINFORMATION, *De Securitate et Defensione* 1 (2022), 17–29, https://doi.org/10.34739/dsd.2022.01.02.

Kuczyńska-Zonik, Aleksandra, Rosyjska dezinformacja i odporność społeczna w państwach bałtyckich, *Komentarze IEŚ* 560/72, (2022), https://ies.lublin.pl/komentarze/rosyjska-dezinformacja-i-odpornosc-spoleczna-w-panstwach-baltyckich/.

Kupiecki, Robert, Bryjka, Filip, Chłoń, Tomasz, Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie, Wydawnictwo Naukowe Scholar, Warszawa 2022.

Lietuvos Respublikos valstybės saugumo departamentas, 2014 *M. VSD VEIKLOS ATASKAITA*, https://www.vsd.lt/wp-content/uploads/2017/03/Veiklos-ataskaita-2014.pdf, retrieved: 05 August 2024.

Lietuvos šaulių sąjunga, Šauliai jungiasi prie iniciatyvos demaskuok.lt ir rengiasi kovai su dezinformacija, https://www.sauliusajunga.lt/sauliai-jungiasi-prie-iniciatyvos-demaskuok-lt-ir-rengiasi-kovai-su-dezinformacija/?fbclid=IwY2xjawEZaLZleHRuA2FlbQIxMAABHdHZiIH-vnmqwCjRjHOs-c2sFbmw-9Pq-khPyx4k8Far5XE7t7RV3-PhsA_aem_GPjo354XOqSPubjToNn1og, retrieved: 13 September 2018.

Lrt.lt, Rusiškos ir baltarusiškos valstybinės žiniasklaidos draudimas: Seime pasigirdo kaltinimai cenzūra, bet pirmas žingsnis žengtas, https://www.lrt.lt/naujienos/lietuvoje/2/1780628/rusiskos-ir-baltarusiskos-valstybines-ziniasklaidos-draudimas-seime-pasigirdo-kaltinimai-cenzura-bet-pirmas-zingsnis-zengtas, retrieved: 15 September 2022.

Lrt.lt, Lietuva ir EBPO steigia unikalią tarptautinę dezinformacijos užkardymo programą, https://www.lrt.lt/naujienos/lietuvoje/2/2248633/lietuva-ir-ebpo-steigia-unikalia-tarptautine-dezinformacijos-uzkardymo-programa, retrieved: 12 April 2020.

Musiał-Karg, Magdalena, Łukasik-Turecka, Agnieszka, Disinformation in the media space during the war in Ukraine. How did Kremlin's fake news blame Ukraine, the USA and NATO for the invasion, (in:) The War in Ukraine. (Dis) information – Perception – Attitudes, eds. M. Musiał-Karg, N. Lubik-Reczek, Peter Lang Verlag, Berlin (2023), 13–38.

Nehring, Christopher, Russische (Des-)Informationspolitik. Bruch oder Kontinuität?, „*Zeitschrift für Außen- und Sicherheitspolitik*" 10 (2017), 441–451, https://link.springer.com/article/10.1007/s12399-017-0672-7, retrieved: 05 August 2024.

NATO, NATO's approach to countering disinformation: a focus on COVID-19, https://www.nato.int/cps/en/natohq/177273.htm, 2020, retrieved: 05 August 2024.

nksc.lt, Nacionalinis kibernetinio saugumo centras: veikla, 2023, https://www.nksc.lt/veikla.html, retrieved: 01 January 2024.

Salomaa, Saara, KAVI's media education supporting democracy, social resilience and comprehensive security, 2024, https://medialukutaitosuomessa.fi/en/kavis-media-education-supporting-democracy-social-resilience-and-overall-security/, retrieved: 24 July 2024.

UKEN, Elfy przeciwko rosyjskim internetowym trollom, 2020, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/10/elfy-przeciwko-rosyjskim-internetowym-trollom/, retrieved: 10 March 2020.

Wardle, Claire, Derakhshan, Hossein, Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, 08. 2018, 2nd revised edition, 2017, https://rm.coe.int/information-disorder-report[1]version-august-2018/16808c9c77, retrieved: 24 July 2024.

Wasiuta, Olga, Wasiuta, Sergiusz, Kremlin Disinformation on the Internet and the Reaction of Western Societies, „*Przegląd Geopolityczny*" 34 (2020), 136–147.

Wilno.tvp.pl, W maju litewska armia wykryła 95 przypadków dezinformacji dot. kwestii obronności, https://wilno.tvp.pl/70603224/w-maju-litewska-armia-wykryla-95-przypadkow-dezinformacji-dot-kwestii-obronnosci, retrieved: 16 June 2023.

Wilno.tvp.pl, Sejm Litwy może uznać manipulacje internetowe za przestępstwo, https://wilno.tvp.pl/68270091/sejm-litwy-moze-uznac-manipulacje-internetowe-za-przestepstwo, retrieved: 03 March 2023.

15min.lt, Ekspertai nagrinėja dezinformacijos grėsmę: lietuviai įsitikinę, kad melagienas reikia pažaboti, 2024, https://www.15min.lt/verslas/naujiena/mokslas-it/ekspertai-nagrineja-dezinformacijos-gresme-lietuviai-isitikine-kad-melagienas-reikia-pazaboti-1290-2223712?utm_medium=copied, retrieved: 12 April 2024.

MANAGEMENT IN DIGITAL TIMES

Edited by Piotr Olaf Żylicz

Vol. 1 Krzysztof Kasianiuk / Bohdan Szklarski / Piotr Olaf Żylicz (eds.): Failed Leadership. 2021.
Vol. 2 Piotr Olaf Żylicz / Vartika Dutta / Rathish Bhatt: Mapping Manager Development. Current and Upcoming Trends. 2023.
Vol. 3 Krzysztof Wasilewski: Digital Humanities and Digital Skills in the Future of Work. 2025.

www.peterlang.com