The Presence of Cybersecurity Competencies in the Engineering Education of Generation Z

Judit Módné Takács, Monika Pogátsnik

Óbuda University, Alba Regia Technical Faculty
Budai u. 45. H-8000 Székesfehérvár, Hungary,
modne.t.judit@amk.uni-obuda.hu, pogatsnik.monika@amk.uni-obuda.hu

Abstract: In the context of 21st Century work in cyberspace, soft skills, and cybersecurity competencies are essential for young engineers in preparation for a career in engineering. The primary objective of this pilot study is to assess the effectiveness and level of security awareness training in the context of digital literacy education, considering the soft skills, educational experiences, and attitudes of the youth. The research uses an innovative methodology. The questionnaire-based quantitative survey is complemented by an alternative qualitative method. In addition to the measurement of attitudes supported by a focus group interview mixed with an imagery association technique, the level of cyber-competence development of the N=130 participating engineering students will be measured by a partially adapted questionnaire. The results of the research will provide insights into the level of awareness, knowledge, and ways of dealing with cyberspace threats among young engineering students, as well as highlight the gaps and strengths of education in terms of skills development. In conclusion, although young engineering students are aware of cyberspace threats, they are not well equipped to deal with them, especially in terms of password habits, security settings, and the use of online social platforms.

Keywords: cybersecurity; education; generation z; competency

1 Introduction

Security awareness combines technical aspects of security with motivations, emotions, behavior, culture, and fears [1]. The term cybersecurity has been coined for the definition of the relationship between cyberspace and security [2]. Nowadays, people need to be prepared and informed about the cyberworld in their personal and professional lives because cyberspace has become an integral part of our lives. Probably due to cost efficiency and changing habits, the communication channel for people in the 21st Century is increasingly shifting to cyberspace [3]. Cyberspace has become part of people's everyday lives, alongside the real, physical world. Like the mechanisms in physical space that have ensured human survival

over thousands of years of evolution, our cybersecurity awareness and protection mechanisms in online space are constantly evolving [4].

A key issue in cyberspace is that people often know enough about cyberthreats to answer certain questions, but they don't know how to apply them in practice [5]. The number of data breaches is increasing rapidly, according to recent trends and cybersecurity statistics [6]. Flexible working has become the norm. 84% of employees can work from home at least part-time. In addition, more than half of employees say they would consider a change of job if they could no longer do their job remotely [7]. Cyberattacks are not only aimed at organizations but also at individuals who work from home or who use unfamiliar software to take part in online meetings [8]. And if someone is not aware of the security of their own devices and systems in cyberspace, it is reasonable to assume that the same user will not be aware of the security of their workplace [9]. The level of security awareness at work is not always the same as at home. Whereas the workplace has multiple levels of control, the home has none, and failures in the home, such as social engineering attacks, present a very serious threat to corporate security [10]. Preventive measures, particularly training, and awareness-raising, are essential. Raising security awareness will lead to higher security of information systems.

As awareness is a combination of motivational, emotional, behavioural, and cultural aspects of security, developing cybersecurity awareness is critical in the field of cybersecurity. Adequate cybersecurity awareness helps individuals and organizations prepare for cyberthreats and the risks they pose. The development of soft skills is a priority area for the 21st Century, given their key role in human relations, communication, and problem-solving. To effectively develop cyber-security awareness, a combination of different skills and practical knowledge is essential. A review of the literature shows that a multifaceted approach and complex teaching methods are key to successful outcomes in the development of cybersecurity awareness.

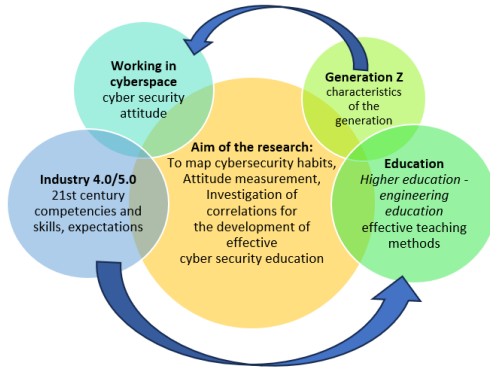

Figure 1

An experimental research strategy for digital education that effectively develops 21st Century skills

Source: Author's construction

With a particular focus on the link between industry and education in the development of digital skills, this research aims (see Figure 1) to explore how the development of cybersecurity awareness, a digital skills cluster, can be integrated into public education from a student's perspective. In addition, the research will analyze the impact of other soft skills that influence the level of cybersecurity awareness, as well as develop a measure to assess the level of cybersecurity awareness among students. The research will also look at the impact of the teaching methods used on the development of cybersecurity awareness. Our aim is to investigate the skills that underpin cybersecurity awareness and to look for correlations between the skills and the effectiveness of the educational methods. The project aims to measure the cybersecurity awareness of students entering university through a pilot, complex, and specific skills evaluation. The research questions are as follows:

Q1: How does developing cybersecurity awareness in public education relate to industry and education in supporting the skills needed for the 21st Century?

Q2: How do soft skills and pedagogical methods are used to influence the development of cybersecurity awareness, and what's the relationship between developing skills, using pedagogical methods, and students' cybersecurity awareness?

Regarding the structure of the article, Chapter 2 analyses the emergence of cybersecurity awareness development in education, analyzing the industry's expectations in the labor market to perform working processes efficiently and safely in cyberspace. The methodology of the experimental research and the innovative combined methods used to measure cybersecurity attitudes are presented in Chapter 3. Chapter 4 details the quantitative survey results and Chapter 5 presents the qualitative focus group interview results using associative methods. Chapter 6 provides a comparison of the research findings with the literature and answers the research questions. Finally, a summary of the research and recommendations for future research directions are provided in Chapter 7.

2 The Importance of the Development of Cybersecurity Awareness in Education in the Light of the Industry

Due to the rapid development of digital transformation in the industry, the development of cybersecurity awareness plays a crucial role in education. The risk and complexity of cyberthreats are increasing with the rise of digitalization and information technologies in the industrial sector. To ensure that students, pupils, and employees are adequately aware of cybersecurity, educational institutions, and professionals need to actively engage in cybersecurity education and training. All

disciplines need to be developed with this in mind, not just focusing on training cybersecurity professionals. Furthermore, modern teaching methods and interactive learning approaches are essential to developing effective cybersecurity awareness and soft skills.

2.1 Reviewing Cybersecurity Skills and Attitudes Related to Industry 4.0/5.0

Cybersecurity has become a fundamental issue for the industry in the 21st Century [11] with the emergence of the Industrial Internet of Things (IIoT), where many smart devices are connected to the web, computers, and people. Cybersecurity skills are a complex, diverse, and long list. Relevant cybersecurity skills and attitudes toward digital competence and the labor market are reviewed below. Digital competence is one of the 8 key competencies of the European Union Reference Framework [12]. Security, including cybersecurity, can be seen as part of digital competence, although its importance has been heightened by the pandemic period. In the present era, the stage of human life has shifted towards cyberspace (work, education, economic sector) [10]. Some terms, for example, have recently gained prominence, such as online education, digital curriculum, industry 4.0, and home office. Industry 4.0 stakeholders have identified a range of skills gaps in digital and cybersecurity (data security, cyberattacks, secure communications, ethical hacking, mobile security, and legal issues) [13]. The shortcomings include low levels of applied digital literacy [14], [15], insufficient critical and analytical thinking [16], lack of ability to adapt to new situations, low flexibility, and resilience [17], and weak cybersecurity skills [18], [19]. Concern about occupational health and safety has been expressed by the European Economic and Social Committee [20]. Digital development is associated with a high-level of psychosocial risks in the workplace, such as work overload, inadequate communication, and an increase in work intensity [21]. A decrease in the sense of security at work and an increase in sources of stress are among the negative effects of digitalization.

2.2 The Education-Job Market Relationship and the Role of Cybersecurity

Companies already need employees who can adapt flexibly and continuously to complex needs because of Industry 4.0 and digitization [22]. Those who can successfully adapt and keep up with the very fast pace of digitalization will be able to prevail. Organizational security training will be successful if it is the creation and improvement of security for all employees within the organization [23]. The demand for cybersecurity professionals is growing. Education cannot currently fill the shortage of skilled labor. In addition, an increasing number of studies and surveys indicate that women are under-represented or under-skilled in STEM and

cybersecurity occupations. In 2021, only 11% of the global cybersecurity workforce will be women, according to one study [24], down from the current expectation of 50%. A 2020 study [25] reported similar results, with 30% of cybersecurity workers under 30 years old being women, 24% in the 30-38 age group, and only 12-14% in the 39-60 age group. The increased involvement of women in cybersecurity will only increase with the growing demand for cyber-security and the general shortage of professionals. However, research shows that men are more aware of cybersecurity and have more favorable habits than women, [26] [27] so women are considered a kind of risk factor in the field of cybersecurity. The factors influencing the development of the necessary skills must therefore be considered in education. There is a close relationship between security awareness at the level of the organization and security awareness at the level of the individual [25].

Generally, a cybersecurity professional is responsible for the organization's, company's, and employees' security in cyberspace. They are constantly checking that the systems in use are operating securely. Training employees, sharing experiences, and raising security awareness are also part of their job. They need to keep up to date with the latest trends in cyberattacks and train themselves continuously. This is just a short list of the responsibilities of a cybersecurity officer, who often needs a lot of soft skills as well as digital skills, a lifelong learning attitude, motivation, and commitment. A high-level of stress tolerance and problem-solving skills are essential, as is the ability to work in 'emergencies'. Good social skills, the ability to adapt to the needs and attitudes of colleagues, and flexibility are important in carrying out tasks in cooperation with all employees of the organization. The ability to react quickly, analytical thinking, and continuous learning is essential in this field due to the emergence of ever-changing technologies and innovations. These multidisciplinary skills are the keys to the success of cyberspace professionals; they are the "Swiss army knives of the digital world".[28] Future workers must be prepared for the consequences of the widespread introduction of new technologies, in particular robotics, high-levels of automation, and the malicious use of artificial intelligence and machine learning, through education, training, and skills development. This includes aspects such as cyber-attacks, system vulnerabilities, data manipulation, hacking autonomous systems, and the mass collection of personal data, which are paramount to security.

2.3 Presence and Development of Digital Literacy and Security Awareness in Education

Since 2013, the development of security awareness from primary school to higher education must be integrated into the educational process of developing IT and digital competencies, as already stated in the Hungarian Government Decree 1139/2013 (III.21.) on the National Cybersecurity Strategy [29]. Promoting the development of cybersecurity competencies is one of the most important areas of higher education, according to a 2016 research report commissioned by the Swiss

Federal Department of Foreign Affairs (FDFA) [30]. Developing online hygiene and safety competencies in education and protecting minors from cyberabuse and radicalization is a focus of the European Commission's Communication on the Digital Agenda for Education 2018 [31]. 1163/2020. (IV.21.) The Government Decision on the National Security Strategy of Hungary states that the main task concerning cyberspace in the country, in addition to the identification and monitoring of actual risks and threats, is the promotion of security-conscious behavior among users [32]. In this way, cybersecurity education has become one of the defining fields of the 21st Century. Cybersecurity education aims to develop the competencies and skills necessary for effective participation in the online environment. The development of appropriate and targeted cyber security education and awareness can make a significant contribution to the prevention of cyberthreats [33]. By raising awareness, security costs can be reduced and the risks to which users are exposed can be minimized. As behavioral culture plays an important role in the development of security awareness [34], parental and teacher awareness is crucial in the education sector. Cybersecurity can be improved, and cyberthreats can be more effectively prevented by actively involving users in awareness raising [35].

Children have access to information and communication technology (ICT) tools even before the school age. The European Commission has published its new Digital Agenda for Education 2021-2027 [36], which defines two strategic directions. Improving the performance of the digital education ecosystem, including the development of the necessary infrastructure, further developing, and strengthening the digital skills of educators [37], as well as securing educational platforms and facilitating the use of high-quality educational content, are key priorities for the coming years.

Education's focus on knowledge transmission is hindered by limited ICT tools and opportunities, hindering students' access to up-to-date knowledge. Students need to enter the world of work with the attitudinal and competency skills to engage in continuous self-improvement, deal flexibly with possible barriers, and maintain motivation for informal learning [38]. School infrastructure is key to developing digital literacy, but access is currently limited to laptops, computers, and projectors. Technological advances such as smartboards, Lego robots, and VR glasses could help improve competence [39]. According to the 2019 OECD Survey, 39% of educators feel minimally prepared to use digital technologies. More than 20% of young people lack basic digital literacy skills [21]. There are gender differences based on the OECD 2022 survey. Research shows that boys on average get higher marks and achieve more than girls [40]. The aim of education is not only the transfer of knowledge but also the development of skills and the raising of awareness.

Correlations between the different levels of digital literacy were one of the findings of the 2020 survey [41] on the digital literacy of teacher educators. For example, the levels of digital literacy and reflective literacy were strongly correlated among respondents. Digital literacy alone is not sufficient for an adequate training process

according to the expectations of the 21st Century, so cross-competences and different skills need to be examined together.

The generational needs of the information society and young people cannot be met by outdated educational methods and conservative educational approaches. Although the national curriculum has prioritized the development of digital literacy since 2007, it can still be seen as an area to be developed in today's classrooms [39]. A lack of cybersecurity awareness and sometimes poor teacher motivation, teaching methods, and digital literacy are also major problems in quality public education [35]. Different levels of education focus on developing online and digital competencies and skills to participate effectively in the online world [42]. Teaching cybersecurity can be challenging when most teachers lack skills, methodologies, and tools. Summarising, the adequate development of students' digital literacy requires qualified teaching staff with digital skills, digital pedagogy, continuous learning, and self-improvement, adequate institutional support through infrastructure and training, and an understanding of the changing roles of students. This will address both technical and behavioral issues to reduce digital illiteracy. [37]

2.4 Generation Z's Digital Literacy and Cybersecurity Awareness and their Measurement in Education Settings

The Youth Digital Skills Index (yDSI) [43], a unique internationally validated measure, was developed based on the following skills dimensions. Technological, operational, and engineering competencies, information navigation and processing competencies, communication and interpersonal competencies, and content generation competencies. The ySKILLS measurement tool was deficient in problem-solving skills, a dimension of digital literacy that has been identified in other studies but is not included in the ySKILLS concept [44]. Among other things, problem-solving skills, which were not included in ySKILLS, are included in the digital skills measurement tool developed by DigComp. DigComp [45] is a self-assessment tool designed to guide individual users in learning and improving. The framework identifies 5 domains of competence (information literacy, communication/collaboration, digital content creation, security, and problem-solving). Under security, it tests skills to protect identity, personal data and privacy, data security, and digital identity [12].

In higher education, and subsequently, in the labor market, the existence and need for cybersecurity skills and cybersecurity awareness is changing [46]. The number of attacks on businesses is increasing every year, with very serious financial consequences [47]. Remote working has had an impact on all sectors of the economy. Cybersecurity skills for almost all workers who use ICT tools in some ways have therefore become important, not just in specific IT security areas. Prevention is the most effective tool, and appropriate education, skills development, and awareness raising are the only way to ensure that a sufficiently skilled and

aware workforce will enter the labor market [48]. Since the principle of security by design can be seen as a preventive technique in the design of modern industrial systems [49], a new approach to engineering education is particularly important. Generation Z grew up in the digital age and is highly digitally literate. However, they do not always have a sufficient level of cybersecurity awareness, which is necessary for them to behave safely in the digital environment. Developing and measuring cybersecurity awareness has become a priority in the educational environment. Frameworks for measuring digital literacy and cybersecurity awareness are presented in yKILLS and DIGCOMP.

3 Purpose and Methods of Research for an Experimental Cybersecurity Skills Assessment

To measure the effectiveness of cybersecurity competence development integrated into IT education, qualitative and quantitative data were collected among a small group of first-year BSc engineering students.

3.1 Aim and Methodology of the Research

The research focuses primarily on the skills of students, the skills that 21st Century workers need. It focuses on security awareness, cybersecurity knowledge, and habits within digital competencies. The direction of inference is inductive. The correlations between cybersecurity competencies and soft skills and the relationship between the methodology of teaching these skills and the cases identified in the pilot research can be used to formulate hypotheses. The reliability of the survey is dependent on the combination and validity of the techniques employed. The use of combined methods is paramount, as no single research method alone can provide complete and reliable results, especially when measuring attitudes [50]. Using mixed methods allows researchers to use multiple data sources, approaches, and analyses to confirm and better understand findings on an issue [51]. The full complexity of the behavior or habit being studied cannot be captured by a single measurement or research method. Ensuring the reliability of research findings requires examining and evaluating the collected data and findings from different perspectives and using different methodologies. Such methodological diversity adds to the validity and reliability of the research so that the research findings can be considered more reliable and comprehensive. [52]

The research relies on the use of paper-based questionnaires and random sampling. A total of 130 first-year undergraduate engineering students were participants. Responses to self-report questionnaires should be treated with caution, as they may not reflect true habits and reality in the case of inadequate self-awareness. Due to the self-reflective nature of the questionnaire, a face-to-face focus group discussion

is justified from a research perspective [51]. The research was complemented by a focus group discussion with an interpretive photo interview [50]. The selection of participants for the focus group discussion was among the respondents to the questionnaire. Six students were selected at random to participate in the focus group. Their habits in cyberspace, which were the focus areas of the questionnaire, were evaluated. The creative and interactive technique used in the focus group discussion helps the interviewees to express their hidden thoughts and spontaneous answers in a freer way. The image association technique makes the interview process more effective and helps the respondents to understand the interview by using an alternative approach.

3.2 Quantitative Research - Self-Reflection Questionnaire

The skills assessment part of the questionnaire was modeled on existing DigComp [45] and yDSI [44] framework survey tools. The questions focus on cyber-security awareness, with some rephrasing and addition of questions from existing questionnaires. The result is a 40-item self-reflection questionnaire that contributes to the understanding of the effectiveness of the preventive education process in terms of digital literacy, security awareness, and cybersecurity skills acquisition. The aim of the questionnaire is not only to measure skills but also to explore the diversity of education methods and sources of knowledge acquisition. The soft skills of the students are also measured by the questionnaire. The questionnaire consists of explicit, closed-ended questions, using a 6-point Likert scale that requires a certain degree of separation from the interviewee. A score of 1 means 'strongly disagree', a score of 4 means 'strongly agree' and a score of 2-3 means 'tend to disagree' - 'tend to agree'. 5 means "I don't understand the question, I don't know what it means" and 6 means "I don't want to answer". Response category 5 represents both inadequate skills and inadequate knowledge.

3.3 Focus Group Interview with Image Association Technique

The relevant research methodology of the focus group discussions is content analysis [53], so this was also chosen in this research. The research questions were summarized in the form of alternative qualitative research to deepen the research. The focus group discussion is conducted using an interpretive photo interview, and image association technique. The subjects of the focus group discussion, 6 persons (1 female, 5 males in gender distribution), were selected randomly from the questionnaire survey. The focus group discussion searches for answers to the attitudes, skills, and competencies of Generation Z youth in cyberspace. The discussion also reveals the methods that teachers used in the previous secondary and primary education processes to help students acquire competencies that they had already gained or even lacked. The image association technique is used as a way of stimulating and motivating reflection on the topic [50]. Verbal questions are

followed by viewing photos and images, followed by a spontaneous interpretation. It is used to support human attitudes, the way individuals think, and the accurate and detailed collection of their experiences.

4 Results of the Cybersecurity Competency Assessment

The results obtained from the questionnaire were subjected to descriptive statistics, looking at the average scores and the distribution of the data. The demographic composition of the sample is 88% male (N=114) and 12% female (N=16), with women underrepresented in our sample. The presented pilot research results are, therefore, not generalizable due to the sampling method used. The survey studied the types of the educational background of the participants. In terms of the percentage distribution, 32% of survey participants entered engineering higher education from general education and 25% from technical secondary school, so 1/4 of them were able to study an engineering subject in-depth during their secondary education. Examining the educational background of the survey respondents and the field of their previous education, slightly more than 50% of the students who were admitted had some type of prior technical education. Figure 2 presents the results for each skill group based on the average of all survey respondents, highlighting the larger negative differences in the areas of safety, stress management, and group.

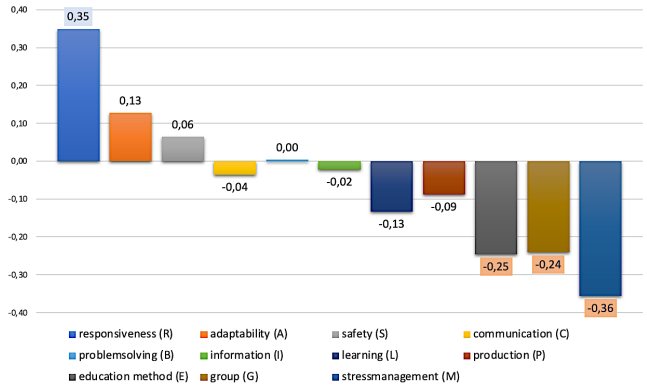

Figure 2

Results for each skill group averaged across survey respondents Source: Author's construction

Participants self-reported performing exceptionally well on the rapid response questions but underperformed in several areas. One critical group is the area of stress management. Figure 2 shows that among the areas that are more strongly below the second and third averages are the ability to work in groups and to evaluate

experienced teaching methods. Categorizing the skills tested, the best mean score=2.01 is for safety skills, while the lowest mean score=1.76 is for teaching and learning skills. The results of the focus group discussion presented later are consistent with these results. The interviews reveal a definite problem with the teaching methods used, which are ineffective and students report having limited support in learning to understand their learning habits and to apply appropriate methods. The Bartlett test and the KMO (Kaiser-Meyer-Olkin) measure were used to check that the conditions for factor analysis were met. The value of the KMO measure was 0.622. The result of Bartlett's test was statistically significant ($\chi 2$ = 911.684, df = 351, $p < 0.001$), indicating a significant difference between the variances of the responses to the cybersecurity awareness questions. Different correlations between statements indicating cybersecurity awareness were found based on the results. Awareness of the ability to block unsolicited pop-ups and attention to the consequences of online activity were negatively correlated (r=-0.315). A positive correlation was found between the awareness of the use of copyright-protected content and the knowledge of copyrights and licences (r=+0.512). There is also a positive correlation between awareness of security settings and awareness of the protection of sensitive data (r=+0.585) and between awareness of trustworthy websites and knowledge of security settings (r=+0.596). Finally, there is a positive correlation between the useful knowledge of cyber-security acquired during the IT training and the attention paid to the security of the Internet (r=+0.606).

In the rest of the research, the article examines in more detail the different aspects of safety skills and their interrelationships. In terms of the scope of the questions, a total of N=3510 evaluable responses were received from participants during the data collection. The following characteristics are collected in Table 1.

Table 1

Summary table of the different distributions of security and cybersecurity issues

Source: Author's construct based on the answers to the security questions of the self-reflection questionnaire (N=3510)

	Absolute frequency distribution	**Relative frequency distribution**	**Cumulative frequency distribution**
	f(a)	***f(%)***	***f(c)***
0 - not	284	8,09	284
1 - rather not	632	18,01	916
2 - rather yes	1208	34,42	2124
3 - yes	1321	37,64	3445

Analyzing further the safety skills of the respondents, the results of female participants (Mean=1,99 Mode=3 Std. Deviation=0,938) and male respondents (Mean=2,04 Mode=3 Std. Deviation=0,948) do not show significant differences, apparently not affected by gender in terms of safety skills and related habits.

From a different perspective, the questions can be divided into two broad domains, the emotional, physiological, and environmental aspects, and the engineering and technical aspects. The safety aspect also shows no significant difference in the respondents' results when the questions are divided into groups. The results for the emotional, physiological, and environmental aspects (mean=2.07 mode=3 std. deviation=0.967) and the engineering and technical aspects (mean=2.00 mode=3 std. deviation=0.922) are almost identical. Categorizing the responses to the survey, the deviation from the mean and standard deviation of the security responses indicates that students in business, public administration, and law performed exceptionally well overall. Additionally, students in STEM and Arts and Humanities were particularly outstanding for safety questions related to emotional, physical, and environmental aspects. Figure 3 shows the correlation coefficients between cybersecurity awareness, soft skills, and the effectiveness of education methods.

		safety	softskill	edu
safety	Pearson Correlation	1	,792**	,665**
	Sig. (2-tailed)		,000	,000
	N	130	130	130
softskill	Pearson Correlation	,792**	1	,666**
	Sig. (2-tailed)	,000		,000
	N	130	130	130
edu	Pearson Correlation	,665**	,666**	1
	Sig. (2-tailed)	,000	,000	
	N	130	130	130

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 3

Correlation between each skill Source: Author's construction

A Pearson correlation was conducted to determine the relationship between cybersecurity awareness, soft skills, and education, and learning skills. A strong positive correlation was found between security awareness and soft skills. This correlation is statistically significant ($r = 0.792$, $n = 130$, $p < 0.01$). This means that participants' cybersecurity awareness is reciprocally enhanced by more advanced communication, problem-solving, and collaboration skills. There is also a moderately strong positive correlation between awareness and education ($r = 0.665$, $n = 130$, $p < 0.01$), meaning that knowledge and skills acquired through innovative teaching methods and appropriate learning skills contribute to cybersecurity awareness development.

5 Interpretative Focus Group Photo Interview Results

Content analysis was used to analyze the results of the focus group interviews. The research involved interviewing six respondents, and the interviews were mixed using an associative technique to enhance the dynamics of the conversation. The interviews were recorded and then transcribed. The transcripts included the interviewees' responses to the research questions. The survey included open-ended questions focusing on online threats, how to set and use security when browsing, how to protect and set personal devices, and how to share information on the Internet. In addition, the survey covered the useful cybersecurity knowledge that was acquired during the studies and its practical use, as well as the educational methods and approaches. The research aimed to get a comprehensive picture of the respondents' cybersecurity awareness and behavior online, as well as the role of education in developing cybersecurity knowledge. Content analysis involved categorizing the responses given based on the questions asked, and then evaluating these categories and their relationships. The choice of methodology allowed for a deeper understanding of the students' opinions, attitudes, and experiences [52]. Participants enjoyed sharing their own experiences but tended to share the experiences of others. The pictures were a great help in revealing deeper thoughts and connections, they were happy to turn to the pictures for help when they got stuck or found it difficult to open up about the topic.

According to the results of the reflective questionnaire, respondents are generally aware of the dangers of cyberspace, but this awareness was only partially confirmed during the focus group. They consider cyberbullying to be the most dangerous form of bullying, but they also recognize that people of all ages can be at risk. Respondents are aware of software that can protect them from threats, but they do not actively use these solutions because they do not have a strong sense of threat. In general, they don't use many security settings in the equipment they use. Biometric identification, anti-virus software, and ad blockers are sometimes used on the computer or mobile phone, but no other protective measures are installed. Based on the data collected in the interview, chat apps, online friends, online dating, collecting likes, Facebook, sharing personal data, manipulation, anonymity, gender neutrality, and Tinder are the aspects that influence the preferred information-sharing habits of Generation Z. The online space is of particular importance to them because of these social interactions, especially the social networking sites that they use. They want to make themselves visible in cyberspace, although they are careful about whom they share content with.

The quantity and quality of the educational process and knowledge transfer was the second area of research identified during the interviews. They had not received any useful cybersecurity knowledge in their classes, although some of them had attended technical secondary schools. They lacked useful knowledge about

cybersecurity, information security, and defenses. They learn about various incidents and defenses from the news. Most of their existing knowledge and skills were gained from personal experience. Students encountered few methodological innovations during the interview. When it comes to pedagogical methods, they experienced traditional pedagogical methods while studying, and sometimes they were only taught using innovative, modern methods. They believe that they will need to learn throughout their lives to be successful and that internal motivation will be particularly important in the future. Money and multiple career opportunities are their motivators for learning. There was a clear desire for a change in the way people were taught, a need for a different, more practical way of teaching, and a reduction in the amount of theoretical knowledge they had been taught.

6 Discussion

Based on the results of the research, it can be concluded that developing cybersecurity awareness in public education is significantly related to industry in supporting the skills needed in the 21st Century. Cybersecurity education and awareness in educational institutions effectively contribute to developing students' digital literacy and security awareness. Gen Z students place a high value on the labor market benefits of a degree while showing little interest in new learning opportunities. When it comes to getting a good job, they consider the importance of relationships and confidence to be paramount. At the same time, the concept of changing people's mindsets, retraining, and lifelong learning is particularly important, as the rapidly changing labor market makes it important for everyone to be prepared for career change and adaptability [54].

Workplace culture affects the effectiveness of responding to cybersecurity incidents, according to 68% of employees [25]. Organizations need to recognize changes in the labor market and adapt to cybersecurity challenges, as workplace culture and employee satisfaction have a significant impact on employee efficiency. Students are motivated by money and career opportunities, thus increasing their learning activities while working and leaving public education. In the coming years, professionals will have to face a shortage of workers and the management of risks generated by new technologies, especially because of working from home [25]. These findings underline the importance of a close relationship between public education and industry to be successful in providing the skills that will be needed in the 21st Century.

Based on the results of the research, it can be concluded that the development of cybersecurity awareness is closely related to soft skills and applied educational methodologies. Defense reflexes and security awareness are already in place for physical threats, but further development is still necessary in cyberspace [9]. Education has a key role to play in raising awareness of cybersecurity, and

experience and practical skills are of key importance for recruits. Relevant IT experience (29-35%), strong problem-solving skills (38-44%), and proper cybersecurity experience (31-35%) are emphasized [25]. There is a lack of response, prevention, and mitigation of already existing problems and attacks. For this reason, in many places, annual training courses, e-learning materials or exams may not be enough to create a real awareness of security [10]. Findings indicate that security awareness is strongly positively related to soft skills and moderately positively related to education. Commitment, self-awareness, and the ability to change are the basis for successful self-education, for which students need to be prepared [9].

Soft skills such as stress management, problem-solving, communication skills, working with others, and conflict management should be developed in students when they enter higher education [55] [56]. The students had acquired most of their existing knowledge and skills from their own experience. There were few methodological innovations encountered by the students during the interviews. In terms of pedagogical methods, students reported similar experiences in surveys of similar age groups, where they had experienced traditional pedagogical methods during their learning and in some cases had only been taught using innovative, modern methods [57]. Cybersecurity awareness is also enhanced by the innovative use of teaching methods and appropriate learning skills. Gender does not affect security skills and habits, as further analysis of respondents' security skills shows no significant difference between female and male respondents. This has led to a contradictory result, as based on the results of several studies [26] [58] [59], men are more aware of security issues. Further research with a larger number of participants would be necessary for confirmation or rejection of this finding.

As far as the habits of the generation are concerned, we can confirm the following results. According to a 2021 survey, over 84% of Hungarians participate in social networking sites, the highest rate in the EU [60]. For Generation Z, the online space, especially social networking sites, plays an important role in socializing and sharing information. Chat apps, online friends, online dating, collecting likes, Facebook, sharing personal information, manipulation, anonymity, gender neutrality, and Tinder are the aspects that influence Generation Z's preferred information-sharing habits, according to the data collected during the interview. Because of these social interactions, especially the social networking sites they use, the online space is particularly important to them. Based on the results, it is important to teach cyber-security awareness and soft skills to support a safer online presence for young people.

Summary, Further Research Directions

In the 21st Century, competencies, and skills in the field of cybersecurity are essential for young professionals. The present exploratory pilot study was able to process 130 usable responses through a quantitative method, which already allowed statistical processing of the data, but the results cannot be generalized. The main

objective of the research was to explore the cybersecurity competencies, soft skills, educational experiences, and mindsets of the students.

Based on the research results, it can be concluded that soft skills and applied pedagogical methods are closely related to the development of cybersecurity awareness. Cyber-security awareness shows a strong positive correlation with soft skills, meaning that the more developed the communication, problem-solving, and collaboration skills of the students, the higher their cybersecurity awareness. The research also showed that knowledge and skills acquired through innovative pedagogical methods as well as appropriate learning skills contribute to developing cybersecurity awareness. These findings highlight the role of soft skills and applied pedagogical methods in increasing students' cybersecurity awareness and emphasize the importance of cybersecurity education and learning. There is a clear justification for the continuation of the research in the future, and its results can be useful in promoting the renewal of education.

References

[1] T. Butler-Bowdown, "Psychology in a nutshell 50 basic psychological works" (Pszichológia dióhéjban 50 pszichológiai alapmű), *HVG Könyvek*, 2007

[2] A. Beláz, D. Berzsenyi, "Cybersecurity Strategy 2.0: Issues for strategic cybersecurity governance" (Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései), *Center for strategis and defense studies analyses* (*Stratégiai védelmi kutató központ (elemzések))*, pp. 1-15, 15 p., 2017

[3] M. Alshaikh et al., "Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness", *27th European Conference on Information Systems (ECIS),* Stockholm & Uppsala, Sweden, 2019

[4] A. P. Bodó et al., "Targeted cyber-attacks. Annual training for staff involved in the security of electronic information systems" (Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára), Budapest, Hungary: *Nemzeti Közszolgálati Egyetem*, 2018

[5] A. Szarvák, V. Póser, "Information Technology Safety Awareness – a review of regularly used terms and methods" *15th International Symposiumon Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020:* AIS 2020 Székesfehérvár, Magyarország: Óbudai Egyetem, pp. 107-111, 5 p., 2020

[6] W.-H. So, H. Kim, "A Study on the Online School Violence of Teenagers in Cyberspace", *Asia-Pacific Journal of Convergent Research Interchange*, Vol. 7, No. 1, pp. 105-114, 2021, doi: 10.47116/apjcri.2020.01.10

[7] D. Berzsenyi, “The human side of cybersecurity” (A kiberbiztonság humán oldala), *Nemzet és Biztonság–Biztonságpolitikai Szemle 10.2*, pp. 54-67, 2017

[8] S. Baraković, J. B. Husic, “Cyber hygiene knowledge, awareness, and behavioral practices of university students”, *Information Security Journal: A Global Perspective*, pp. 1-24, 2022, doi: 10.1080/19393555.2022.2088428

[9] I. Dobák, S. Babos, “Security awareness opportunities in the light of 21st Century platforms” (A biztonságtudatosítás lehetőségei a 21. századi platformok fényében), *Nemzetbiztonsági Szemle*, Vol. 9, No. 4, pp. 18-34, 2021, doi: 10.32561/nsz.2021.4.2

[10] R. Gyaraki, “The role of security awareness, or questions about cybersecurity” (A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról), *Magyar Rendészet*, Vol. 22, No. 2, pp. 245-261, 2022, doi: 10.32577/mr.2022.2.16

[11] A. Corallo et al., “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review”, *Computers in Industry,* 137, 103614, 2022, https://doi.org/10.1016/j.compind.2022.103614

[12] EU Science Hub, European Commission, *The Digital Competence Framework 2.0*, 2021, URL: https://tinyurl.hu/33WQ (last retrieved: 2021.10.21.)

[13] P. Leitão et al., “Analysis of the Workforce Skills for the Factories of the Future”, *IEEE Conference on Industrial Cyberphysical Systems (ICPS2020),* Vol. 1, pp. 353-358, 2020, doi: 10.1109/ICPS48405.2020.9274757

[14] N. Soukupová et al., “Industry 4.0: an Employee Perception” (Case of the Czech Republic), *Acta Universitatis Agriculturae Et Silviculturae Mendelianae Brunensis,* Vol. 68, No. 3, pp. 637-644, 2020, doi: 10.11118/actaun202068030637

[15] N. Obermayer et al., “Companies on Thin Ice Due to Digital Transformation: The Role of Digital Skills and Human Characteristics”, *International and Multidisciplinary Journal of Social Sciences,* Vol. 11, No. 3, pp. 88-118, 2022, doi: 10.17583/rimcis.10641

[16] W. Puriwat, S. Tripopsakul, “Preparing for Industry 4.0 - Will youths have enough essential skills?: An Evidence from Thailand”, *International Journal of Instruction*, Vol. 13, No. 3, pp. 89-104, 2020, doi: 10.29333/iji.2020.1337a

[17] N. Obermayer et al., “Influence of Industry 4.0 technologies on corporate operation and performance management from human aspects”, *Meditari Accountancy Research,* Vol. 30, No. 4, pp. 1027-1049, 2022, doi: 10.1108/MEDAR-02-2021-1214

[18] S. Von Solms, L. A. Futcher, "Adaption of a Secure Software Development Methodology for Secure Engineering Design", *IEEE Access,* Vol. 8, pp. 125630-125637, 2020, doi: 10.1109/ACCESS.2020.3007355

[19] F. Iniesto et al., "When industry meets Education 4.0: What do Computer Science companies need from Higher Education?", *TEEM'21: Ninth International Conference on Technological Ecosystems for Enhancing Multiculturality,* pp. 367-372, 2021, doi: 10.1145/3486011.3486475

[20] European Parliament 2021/C 56/02, "Opinion of the European Economic and Social Committee on 'Industrial transition towards a green and digital European economy: regulatory requirements and the role of social partners and civil society' (exploratory opinion)", 2021, URL: https://eur-lex.europa.eu/ (last retrieved: 2022.03.17)

[21] S. Vandekerckhove et al., "Musculoskeletal disorders and psychosocial risk factors in the workplace — statistical analysis of EU-wide survey data, Report", *European Agency for Safety and Health at Work,* Publications Office of the European Union, 2021, doi: 10.2802/39948

[22] B. Fregan, I. Kocsis, Z. Rajnai, "IPAR 4.0 and the risks of digitalisation" (Az IPAR 4.0 és a digitalizáció kockázatai), *Műszaki Tudományos Közlemények (HU) 9:* 1 pp. 87-90, 4 p., 2018

[23] Computerworld, "Cybersecurity is not just an IT problem" (A kiberbiztonság nem csak az informatikusok problémája), 2019, URL: https://tinyurl.hu/OkCd (last retrieved: 2021.08.17)

[24] Cybersecurity Guide, A guide for women in cybersecurity, 2021, URL: https://tinyurl.hu/14Cb (last retrieved: 2021.08.20)

[25] ISC, Cybersecurity Workforce Study: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution, 2022, URL: https://tinyurl.hu/LpqC (last retrieved: 2023.02.14.)

[26] T. Palicz et al., "Results of the 2020 National Population Survey on Security Awareness in Cyberspace" (Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei), *Belügyi Szemle*, Vol. 70, No. 2, pp. 395-418, 2022, doi: 10.38146/bsz.2022.2.11

[27] S. M. Kennison, E. Chan-Tin, "Taking Risks with Cybersecurity: Using knowledge and personal characteristics to predict Self-Reported Cybersecurity Behaviors", *Frontiers in Psychology,* Vol. 11, 2020, doi: 10.3389/fpsyg.2020.546546

[28] Cybersecurity Guide, How to Become a Cybersecurity Specialist, 2021, URL: https://tinyurl.hu/r1m4 (last retrieved: 2021.09.23)

[29] 1139/2013. (III. 21.) "Government Decision on the National Cyber Security Strategy of Hungary" (Kormányhatározat Magyarország Nemzeti

Kiberbiztonsági Stratégiájáról), *Magyar Közlöny Lap- és Könyvkiadó Kft.,* 2013

[30] V. Radunovic, D. Rüfenacht, "Cybersecurity competence building trends Research report Commissioned by the Federal Department of Foreign Affairs of Switzerland", *DiploFoundation,* 2016

[31] European Comission, the European Economic and Social Committee and the Committee of the Regions on the Digital Education Action Plan COM(2018) 22 final, 2018

[32] 1163/2020. (IV.21.) "Government Decision on the National Security Strategy of Hungary " (Kormányhatározat Magyarország Nemzeti Biztonsági Stratégiájáról), 2020

[33] K. Fekete-Karydis, B. Lázár, "Development of cyber defense strategies, cyber defense challenges, current events" (A kibervédelmi stratégiák fejlődése, kibervédelmi kihívások, aktualitások), *HSZ-HDR*, köt. 147, sz. 5, o. 60-72, 2021

[34] R. Stohl, ""How to Train Your Dragon!" – About the training and learning habits of Generation Z" („Így neveld a sárkányodat!" – A Z generáció képzési és tanulási szokásairól), *Honvédségi Szemle – Hungarian Defence Review*, pp. 116-127, 2021, doi: 10.35926/hsz.2021.2.9

[35] Z. Nyikes, "Information security enhancement with user support options" (Az információbiztonság növelése a felhasználó támogatásának lehetőségeivel), Studia Doctorandorum Alumnae II.: Válogatás a DOSz Alumni Osztály tagjainak doktori munkáiból II. Budapest, Magyarország : *Doktoranduszok Országos Szövetsége (DOSZ),* 2021, 964 p. pp. 637-806, 170 p.

[36] European Comission, Digital Education Action Plan 2021-2027, Resetting education and training for the digital age, 2020

[37] Z. Balogh et al. "The impact, characteristics and challenges of digital literacy and digital culture on society and education" (A digitális kompetencia és a digitális kultúra társadalomra és oktatásra gyakorolt hatásai, jellemzői, kihívásai), *Civil Szemle 17:* 2 pp. 69-88, 19 p., 2020

[38] A. Kálmán, B. G. Kálmán, "The impact of industry 4.0 competence requirements on school system education" (Az ipar 4.0 kompetenciaigényeinek hatása az iskolarendszerű oktatásra), *Iskolakultúra*, Vol. 32, No. 12, pp. 57-73, 2022

[39] T. L. Nyitrai, "The home position of teacher digital competence in public education before COVID-19" (A tanári digitális kompetencia helyzete a közoktatásban a COVID-19 előtt), *jATES,* Vol. 11, No. 2, pp. 124-136, 2021

[40] National competence measurement 2022 (Oktatási Hivatal, Országos kompetenciamérés 2022), URL: https://tinyurl.hu/RvR6 (last retrieved: 2023.03.19.)

[41] L. Horváth et al., "Measuring the digital competence of teacher educators - adapting DigCompEdu to the domestic higher education environment" (Tanárképzők digitális kompetenciájának mérése – a DigCompEdu adaptálása a hazai felsőoktatási környezetre), *Neveléstudomány: Oktatás Kutatás Innováció 8:* 2, pp. 5-25, 21 p., 2020

[42] K. Thiyagu et al., "Cyber safety and security education", *Lulu Publication,* 2019

[43] E. J. Helsper et al., "The youth Digital Skills Indicator", *Zenodo*, 2021, doi: 10.5281/zenodo.4476540

[44] E. J. Helsper et al., "The Youth Digital Skills Indicator: Report on the conceptualisation and development of the ySKILLS digital skills measure", 2021, URL: https://osf.io/m84pe/ (last retrieved: 2021.10.21.)

[45] Cs. Kvaszingerné Prantner, "DIGCOMP 1.0 and DIGCOMP 2.0, The impact of culture change on individual competences: models of digital competence" (A DIGCOMP 1.0 és a DIGCOMP 2.0, A kultúraváltás hatása az egyéni kompetenciákra: a digitális kompetencia modelljei), Eger, Magyarország : *EKE Líceum Kiadó*, 143 p. pp. 59-74, 16 p., 2020

[46] J Novák, "Methods to increase safety awareness in higher education" (Biztonságtudatosság növelésének eszközei a felsőoktatásban), *Műszaki Tudományos Közlemények (HU) 9* : 1, pp. 183-186, 4 p., 2018

[47] Cs. Kollár, J. Poór, "Organisations in the digital age - Information security aspects of the digital workplace" (Szervezetek a digitális korban – A digitális munkahely információbiztonsági aspektusa), *Kiberbiztonság - Cyber Security: Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból,* Budapest, Magyarország: Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 366 p. pp. 95-107, 13 p., 2018

[48] Z. Nyikes, "Possibilities for developing security awareness" (A biztonságtudatosság fejlesztésének egyes lehetőségei), *Műszaki Tudományos Közlemények* (HU) 7 pp. 327-330, 4 p., 2017

[49] P. Bóna, "User awareness is the first line of defence" (A felhasználók biztonságtudatossága az első védelmi vonal) - Videó, *Comforth.hu,* 2020, URL: https://bit.ly/3Ek0WGX (last retrieved: 2021.07.08)

[50] D. Horváth, A Mitev, "Alternative qualitative research manual" (Alternatív kvalitatív kutatási kézökönyv), *Aliena Kiadó,* 2015

[51] A. Kelemen-Erdős, A. Á. Mészáros, "Ethics and Social Responsibility of Information Intermediaries in International Businesses", *Arab Journal of Administration* 41 pp. 239-248, 10 p. 2021

[52] Á. Szokolszky, “Research work in psychology: methodology, methods, practice” (Kutatómunka a pszichológiában: metodológia, módszerek, gyakorlat), *Osiris tankönyvek*, 2004

[53] A. Kelemen-Erdős, “Selection Listing Decisions: New Product Adoption of Food Retailers”, *Journal of Research in Business, Economics and Management 10*: 3 pp. 1905-1917, 13 p. 2018

[54] I. C. Papp et al., “Study preferences in higher education”, *Acta Polytechnica Hungarica*, Vol. 20, No. 4, pp. 229-248, 2023, doi: 10.12700/aph.20.4.2023.4.13

[55] Gy. Molnár, B. Orosz, “Current issues of digitisation processes in a changing digital environment: reflections on some pedagogically relevant contexts in Hungary” (Digitalizációs folyamatok aktuális kérdései változó digitális környezetben: Reflexiók néhány magyarországi pedagógia-releváns kontextusra), Komárno, Szlovákia: *International Research Institute*, 378 p. pp. 120-131, 12 p., 2020

[56] J Módné Takács, M. Pogátsnik, “Examining the stress management techniques of university students” (Az egyetemi hallgatók stresszkezelési technikáinak vizsgálata), *Módszertani újítások és kutatások a szakképzés és a felsőoktatás területén: X. Trefort Ágoston Szakképzés- és Felsőoktatás-pedagógiai Konferencia Tanulmánykötet,* Budapest, Magyarország : Óbudai Egyetem, 424 p. pp. 262-278, 17 p., 2021

[57] G. Farkas et al., “Quality Improvement in Education, based on Student Feedback”, *Acta Polytechnica Hungarica*, Vol. 20, No. 6, pp. 215-228, 2023, doi: 10.12700/aph.20.6.2023.6.12

[58] S. M. Kennison, E. Chan-Tin, “Taking Risks with Cybersecurity: Using knowledge and personal characteristics to predict Self-Reported Cybersecurity Behaviors”, *Frontiers in Psychology*, Vol. 11, 2020, doi: 10.3389/fpsyg.2020.546546

[59] T. McGill, N. Thompson, “Gender differences in information security perceptions and behaviour, in University of Technology”, *Sydney eBooks*, 2018, doi: 10.5130/acis2018.co

[60] EUROSTAT, Digital society statistics at regional level, 2022, URL: https://tinyurl.hu/eOpI (last retrieved: 2023.03.19.)