Online-Journals.org

iJEP International Journal of Engineering Pedagogy

iJEP | eISSN: 2192-4880 | Vol. 15 No. 7 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijep.v15i7.58939

PAPER

Profiling Cross-Generational Cyber Resilience through Scale Development

Judit Módné Takács (✉), Monika Pogátsnik

Obuda University
Alba Regia Faculty,
Székesfehérvár, Hungary

modne.t.judit@amk.uni-obuda.hu

ABSTRACT

This study develops and validates the personal cyber resilience scale (PCRS) to identify resilience profiles and explore differences between Gen Z engineering students and Gen Alpha students nearing higher education. A mixed-methods study (N = 3275) employed EFA, CFA, and K-means clustering, supplemented by qualitative analysis. We developed a robust 32-item, seven-factor PCRS (α = .871) and identified four stable profiles. Profile distribution differed significantly by generation (p = .011) and gender (p < .001), with qualitative data providing context to these differences. The PCRS is an effective tool for measuring youth cyber resilience, and the profiles can inform targeted prevention strategies in educational contexts.

KEYWORDS

cyber resilience, digital natives, scale development

1 INTRODUCTION

Young people in the digital age, particularly Generation Z and Alpha, inhabit an online world where their social relationships, identity, and learning are deeply intertwined with the digital space [1], [2]. While this environment offers numerous opportunities, it also presents serious risks such as cyberbullying, disinformation, data misuse, and exposure to harmful content [3], [4]. To ensure a safe online presence, digital resilience has become increasingly crucial. This capability allows individuals to adapt, recover, and maintain their well-being amidst online threats [5]. Developing emotional resilience is especially important for youth, as they react sensitively to the psychological impacts of cyberbullying and require targeted support [6].

The study of digital resilience is hindered by three main obstacles: (1) the concept is new and lacks a unified definition, often being confused with digital literacy; (2) reliable measurement instruments are scarce; and (3) teenagers, the most active internet users, are the least researched demographic despite their significant need for development [5], [6], [7]. This is particularly relevant for Gen Z students in higher

Módné Takács, J., Pogátsnik, M. (2025). Profiling Cross-Generational Cyber Resilience through Scale Development. *International Journal of Engineering Pedagogy (iJEP)*, 15(7), pp. 69–84. https://doi.org/10.3991/ijep.v15i7.58939

Article submitted 2025-07-09. Revision uploaded 2025-08-15. Final acceptance 2025-09-20.

education, including engineering students, as well as for the Gen Alpha cohort soon entering universities, who face complex online challenges from a very young age.

In response to these challenges, this study employs a multi-phase, mixed-methods approach with two primary objectives. The first is to develop and validate a new instrument, the Personal Cyber Resilience Scale (PCRS). The second is to use this scale to map the cyber resilience profiles of Hungarian youth and to examine generational and gender differences across these profiles and the main dimensions of resilience. Based on the theoretical complexity of cyber resilience and the diversity of youth online behaviours, we formulate the following hypothesis:

H1: *Statistically distinct cyber resilience profile groups, based on patterns of cybersecurity awareness, resilience, and problematic internet use, can be identified between members of Generation Z and Alpha.*

By developing a robust measurement tool, this study aims to provide both a methodological contribution to the field and practical insights into the youngest generations.

2 LITERATURE REVIEW

2.1 Theoretical framework and dimensions of cyber resilience

Sun et al. [5] provide a comprehensive framework defining digital resilience as both a capacity and a dynamic cyclical process that shapes responses to digital stressors. They identified five core dimensions: (1) understanding online threats, including risks like cyberbullying and information overload; (2) knowing solutions and how to seek help; (3) learning knowledge and skills from experiences to adapt future decisions; (4) recovering from stress by returning to a baseline level of functioning after negative online events; and (5) moving forward through self-efficacy, which involves not just recovery but personal growth. This model frames digital resilience as a continuously developing capability [5].

A systematic review by Qamaria et al. [6] further reveals that ecological theory is a dominant perspective in youth cyber resilience research. This approach suggests resilience is shaped by an interplay of internal factors like self-control and external factors like social support. Key skills involve defending against cyberbullying, managing screen time, and critically evaluating information [6].

In summary, the literature highlights the complex and dynamic nature of digital resilience by integrating cognitive, psychological, and behavioural components. Significant research gaps remain regarding adolescents and the lack of validated measurement tools. This study addresses these gaps. We operationalise cyber resilience as a multidimensional construct to develop a reliable and valid instrument for young populations based on these theoretical foundations.

2.2 Challenges in measuring cyber resilience

The empirical study of cyber resilience is hindered by three interconnected methodological issues. These are fragmented measurement approaches, a lack of contextual consideration, and inadequate psychometric validation. The most significant problem is the fragmentation of measurement tools. Components of cyber resilience,

such as cybersecurity awareness, problematic internet use, or general psychological resilience, are typically measured with separate scales. These scales are based on different theoretical backgrounds and validated on diverse populations.

For example, cybersecurity awareness instruments like the scale validated by Bognár and Bottyán [8] or the Cybersecurity Scale (CSA) [9], [10] and its social media version (CSAS) [11] focus on proactive defensive behaviours. Their specific focus on technical practices excludes the crucial psychological and behavioural dimensions of resilience. Conversely, widely used psychological resilience scales such as the Connor-Davidson Resilience Scale (CD-RISC) [12] or the Child and Youth Resilience Measure (CYRM-28) [13] concentrate on general psychosocial coping abilities and are not specific to the digital context. This fragmentation makes it difficult to conceptualise and test a unified, multidimensional model of cyber resilience.

Recent initiatives have begun to address this gap. A notable example is the study by Qi and Yang [14], which introduced a digital resilience scale for Chinese adolescents, based on the identification of four risk factors: 1) knowing the risks, 2) seeking help, 3) proactive learning, and 4) recovery. However, this scale highlights the problem of cultural and contextual embeddedness. An instrument validated in a specific educational and social system like China may not be directly applicable to a European or Hungarian context, where language, slang, and digital communication norms differ.

Finally, a third challenge is the lack of psychometric validation for the youngest generations. Few existing instruments have been specifically validated for the unique characteristics of Gen Z or Alpha. For instance, the CSAS [11] targets a broad demographic of social media users, while the CYRM-28 [13] measures psychological resilience in youth but does not integrate cyber-specific dimensions.

These challenges collectively underscore the urgent need for a new, psychometrically robust, and multidimensional scale. Such an instrument must measure youth personal cyber resilience comprehensively, taking into account the specific traits of Gen Z and Alpha. This study aims to fill this gap by developing and validating a culturally sensitive cyber resilience scale tailored for a young Hungarian population.

2.3 Generational differences in the online space

Understanding the digital habits of Generation Z and Alpha is essential for exploring cyber resilience profiles. The impact of their different digital socialisation experiences on resilience remains an under-researched area, despite their intense online presence [5], [6], [8], [10]. Recent data show that 97% of young people aged 16–29 in the European Union and 99% in Hungary use the Internet daily [14]. This activity occurs within a diverse platform ecosystem, with a majority actively using YouTube (93%), TikTok (63%), Snapchat (60%), and Instagram (59%) [15].

The literature describes this constant navigation between physical and digital worlds as “digital acculturation”, a process where youth must develop competency areas while adapting to online specificities like anonymity and accessibility. The depth of this process is highlighted by the “digital phenotype” concept, which suggests online behaviour can serve as an indicator of an individual’s mental health [16].

The key distinction between the two generations lies in the nature of their digital socialisation. For Generation Z, this process was shaped by peer interactions and identity exploration on social media platforms that encouraged active self-presentation [17]. In contrast, for Generation Alpha, digital devices are not just communication tools but normative mediums for interaction, learning, and play from a

very young age. By age two, 40% of this generation already had a tablet, a figure that rose to 58% by age four [18]. For them, digital devices are how they interact with the world, learn, and play [19]. A systematic review by Höfrová et al. [20] characterises Gen Alpha as more curious and mobile but also more self-centred and irritable, with heightened emotionality.

These differing formative experiences likely shape distinct cyber resilience profiles. For example, the cognitive flexibility of Gen Alpha may support proactive learning, while their heightened emotionality could make them more vulnerable to online stress. Although the literature documents these generational traits, empirical studies examining how they translate into specific cyber resilience dimensions are lacking. This research gap creates a significant opportunity to empirically investigate generational cyber resilience dynamics.

3 STATISTICAL ANALYSIS AND METHODOLOGY

This study employed a multi-phase, sequential explanatory mixed-methods approach. The initial quantitative phase aimed to develop and validate the Personal Cyber Resilience Scale (PCRS) and identify resilience profiles. The subsequent qualitative phase served to provide a deeper understanding of the quantitative findings, particularly the generational and gender differences.

3.1 Participants and procedure

The questionnaire used for quantitative data collection included demographic items and the items for the Personal Cyber Resilience Scale (PCRS). The initial item pool for the PCRS was compiled from relevant items from three validated instruments: the Hungarian adaptation of the Cybersecurity Scale (CSC-H), the Connor-Davidson Resilience Scale (CD-RISC), and the Problematic Internet Use (PIU) scale. This item pool served as the basis for the exploratory factor analysis (EFA) to identify an integrated cyber resilience factor structure.

Data were collected between September 2022 and May 2023 using paper-based and online questionnaires in schools across Fejér County, Hungary, ranging from upper primary school to higher education. After removing outliers, the final sample consisted of $N = 3275$ participants (74.4% Gen Z; 53.3% male). Participation was voluntary and anonymous, with parental and participant consent obtained.

The qualitative phase involved 15 semi-structured focus group interviews with $N = 89$ participants from the surveyed population, ensuring representation from both generations.

3.2 Statistical data analysis

Data processing was conducted using SPSS 27, Excel, and Python (Google Colab) with the pandas, semopy, seaborn, numpy, matplotlib, and sklearn libraries. The Google Gemini 2.5 Pro language model assisted in refining the manuscript's language.

In the first phase, the psychometric properties of the PCRS were examined. Prior to performing an EFA, the Kaiser-Meyer-Olkin measure (KMO > .60) and the

significance of Bartlett's test were confirmed. A Promax rotation was used, and the criteria for item retention were a factor loading > .40 and the absence of significant cross-loadings. One item with a lower loading was retained to ensure the factor's content validity. The internal consistency of the factors was assessed using Cronbach's alpha (α > .60). The model was then validated using a second-order Confirmatory Factor Analysis (CFA) on a 70% training and 30% test split of the sample, evaluated with standard model fit indices (CFI > .90, TLI > .90, RMSEA < .08, SRMR < .08) [21], [22], [23], [24].

In the second phase, K-Means cluster analysis was performed on the Z-scores of the validated factors to identify cyber resilience profiles. The distribution of these profiles by generation and gender was examined using chi-square tests. Differences across the sub-dimensions were analysed with independent samples t-tests and Mann-Whitney U tests (p < .05) [25]. In the qualitative phase, the focus group transcripts were analysed using content analysis and a three-column thematic analysis approach. After segmenting the transcripts into meaning units, inductive coding was applied. These coded units were then organised into higher-level themes to provide a deeper understanding of the experiences, attitudes, and strategies behind the quantitative patterns [26].

4 RESULTS

4.1 The Personal Cyber Resilience Scale

The development of the PCRS involved a multi-step iterative refinement process. Following an item-level analysis and a systematic, theory-driven EFA, an initial pool of 41 items was reduced to a final, robust structure.

The final 32-item scale demonstrated excellent suitability for factor analysis (*KMO* = .896, Bartlett's Test: $\chi^2(496) = 29093.68$, p < .001). The analysis yielded a seven-factor model that explained 56.99% of the total variance and showed excellent overall internal consistency (*Cronbach's* α = .871). Table 1 summarizes the final factor structure of the PCRS, including the abbreviated content of each item, its factor loading, and the Cronbach's alpha for each of the seven theoretically distinct subscales.

Table 1. Factor structure of the Personal Cyber Resilience Scale

Factor and Item	Loading	Cronbach α
1. Proactive Data and Access Protection		**.787**
CSCH01: Cautious about sharing personal information online	.704	
CSCH02: Only share what I'd share in real life	.763	
CSCH03: Ensure data visibility is limited to necessary people	.765	
CSCH04: Don't share contact information online	720	
CSCH05: Don't share passwords with anyone	.674	
CSCH06: Create strong passwords with symbols, numbers, capitals	.457	
CSCH07: Use phone verification for email protection	*.354*	
CSCH08: Answer security questions correctly	.439	

(Continued)

Table 1. Factor structure of the Personal Cyber Resilience Scale *(Continued)*

Factor and Item	Loading	Cronbach α
2. Mental Strength and Self-Control		**.785**
RISC03: I give my best effort regardless of the situation	.637	
RISC04: I don't give up when things seem hopeless	.705	
RISC05: I think clearly and focus under pressure	.677	
RISC06: I see myself as a strong person	.769	
RISC08: I am very goal-oriented	.774	
RISC09: I feel I control my life	.618	
3. Active Technical Defence		**0.809**
CSCH19: Use updated antivirus software	.852	
CSCH20: Regularly scan devices with antivirus	.908	
CSCH21: Keep firewall active	.688	
CSCH22: Scan downloaded files before opening	.694	
4. Cyber Threat Detection		**0.776**
CSCH14: Don't trust emails from unknown senders	.648	
CSCH15: Don't trust websites without security certificates	.551	
CSCH16: Don't open spam emails	.751	
CSCH17: Ignore social engineering emails, phishing awareness	.669	
CSCH18: Avoiding suspicious content, unknown links/attachments	.682	
5. Online Problem-Solving		**0.685**
CSCH23: Use social media for information sharing	.686	
CSCH24: Use cyberspace services to solve problems	.823	
CSCH25: Use cyberspace for information management	.754	
6. Offline Well-being		**0.644**
PIH_02_rev: Try to hide your online time usage	.813	
PIH_03_rev: Feel tense, irritated, or stressed when unable to use the Internet as long as desired	.798	
PIH_04_rev: Feel depressed, moody, or nervous offline, with these feelings stopping once back online	.677	
7. Trust in Online Data Storage		**0.614**
CSCH10: Believe cyberspace data storage is safe	.817	
CSCH11: Trust cloud stored information won't be lost/deleted	.590	
CSCH12: Believe data sharing involves no risk	.802	

Notes: Item content has been abbreviated for clarity. Factors below 0.4 are marked in italics.

The resulting factor structure is considered robust. Most items load strongly (> .50) onto their respective factors, and the majority of subscales exhibit good internal consistency ($\alpha > .70$). The reliability of factors with fewer items (5, 6, and 7) is acceptable ($\alpha > .60$) but indicates potential directions for future refinement, such as expanding these factors with new items to increase their reliability.

4.2 Confirmation and validation of the PCRS factor structure

To test the internal validity and generalizability of the seven-factor structure identified in the EFA, a second-order confirmatory factor analysis (CFA) was conducted. To prevent bias and assess model robustness, the sample was randomly split into a 70% training set and a 30% test set. The model specified a central, second-order latent "cyber resilience" factor that encompassed the seven first-order factors, while also allowing for specific, direct paths between the first-order factors.

Figure 1 displays the final structural model estimated on the training set. The model fit indices indicated an acceptable fit, supporting the validity of the hypothesized structure (CFI = .905, TLI = .895, RMSEA = .043, SRMR = .049).

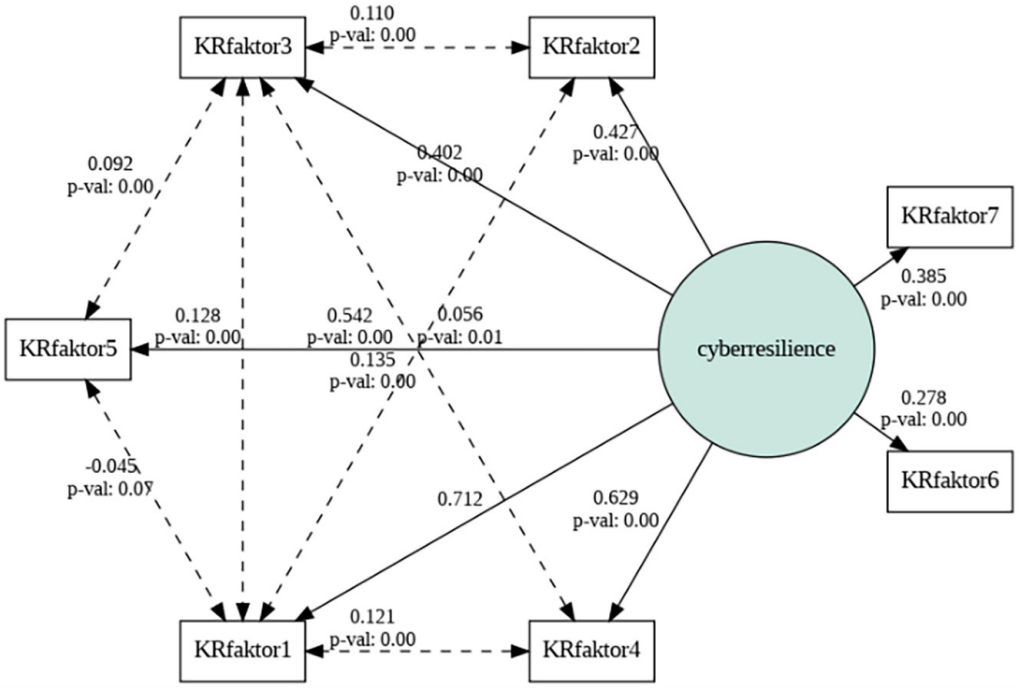

Fig. 1. Structural model of the Personal Cyber Resilience Scale (PCRS) on the training data set, with standardized path coefficients

Notes: Continuous arrows indicate the effects of the central "cyber resilience" factor, while dashed arrows indicate specific, direct paths between first-order factors. All indicated paths are significant ($p < .05$), unless otherwise noted.
Source: Authors' own compilation.

The central "cyber resilience" factor, acting as a general protective factor, significantly and positively predicted all seven sub-dimensions. The strongest effects were observed on proactive data and access protection (Factor 1, $\beta = .712$) and Cyber Threat Detection (Factor 4, $\beta = .629$). A weaker but still significant effect was found for offline well-being (Factor 6, $\beta = .278$). Beyond this general factor, the model revealed several specific pathways. For instance, Mental Strength (Factor 2) directly and positively influenced active technical defence (Factor 3, $\beta = .110$), suggesting that psychological resources facilitate the use of specific technical behaviours.

The model's generalizability was then cross-validated on the test set. As shown in Table 2 and Figure 2, the fit indices demonstrated a modest but expected decline, a natural occurrence during cross-validation. The CFI (.886) and TLI (.875) values fell slightly below the .90 threshold. However, the error indices remained well within the acceptable range (RMSEA = .047 [90% CI: .044, .050]; SRMR = .058).

Table 2. Comparison of model fit indices

Fit Index	Training Set Value	Test Set Value
Chi-Square (χ^2)	2373.07	1419.39
Degrees of Freedom (df)	450	450
p-value (*p*)	< .001	< .001
CFI	.905	.886
TLI	.895	.875
RMSEA [90% CI]	.043 [.041, .045]	.047 [.044, .050]
SRMR	.049	.058

Notes: CFI = Comparative Fit Index; TLI = Tucker–Lewis Index; RMSEA = Root Mean Square Error of Approximation; CI = Confidence Interval; SRMR = Standardized Root Mean Square Residual. Accepted threshold values for good model fit are: CFI and TLI > .90, RMSEA < .08, and SRMR < .08.

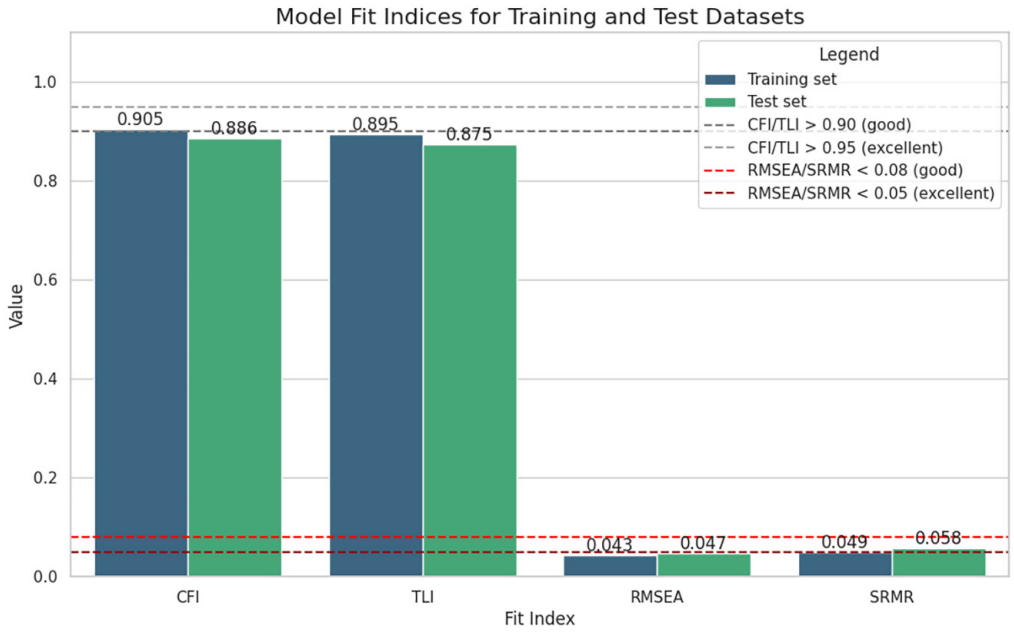

Fig. 2. Comparison of the main model fit indices for the second-order cyber resilience model across the training (exploratory) and test (confirmatory) datasets

Source: Authors' own compilation.

In conclusion, the model demonstrated an acceptable fit on the training data. The slight degradation in fit during cross-validation may suggest minor overfitting, but the stable and low error indices indicate that the model's fundamental structure is robust and generalizable. These results provide cautious but substantial support for the validity of the seven-factor, second-order structure of the personal cyber resilience scale.

4.3 Identification of cyber resilience profiles

To identify distinct cyber resilience profiles based on the seven factors revealed by the PCRS, a K-means cluster analysis was performed. The standardised Z-scores of the seven factors were used as input variables to ensure that each dimension contributed equally to the clustering process.

The optimal number of clusters was determined using the elbow method. As shown in Figure 3, clear inflection points are visible at k = 2, k = 3, and k = 4. After the k = 4 point, the decrease in within-cluster variance (inertia) slows considerably, indicating that adding more clusters would not yield significant improvements in homogeneity. Based on theoretical considerations and the presumed complexity of youth online behaviour, the four-cluster solution was deemed the most interpretable and informative.

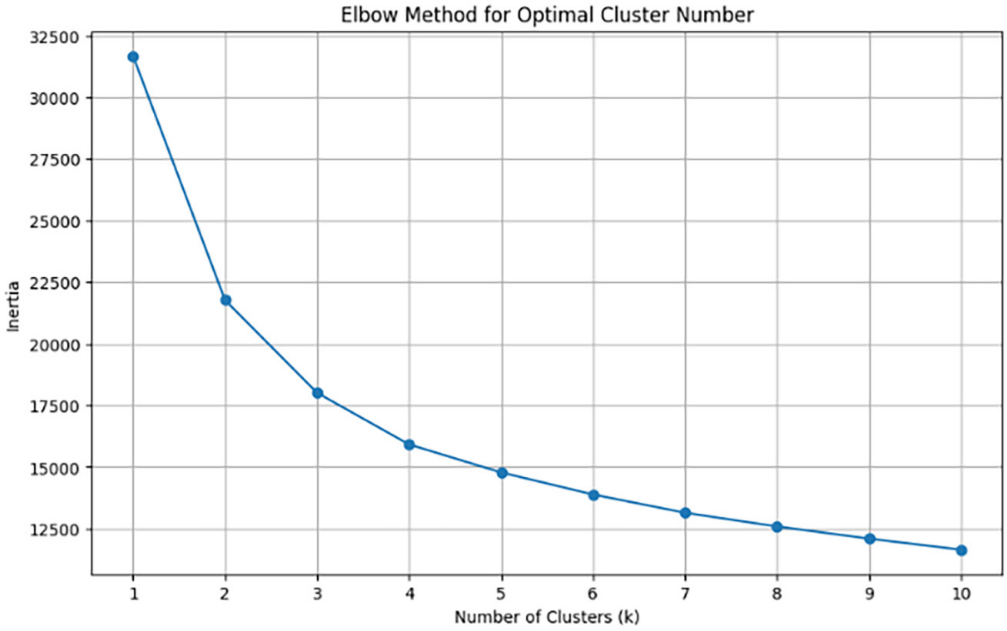

Fig. 3. Determining the optimal number of clusters using the elbow method

Source: Authors' own compilation.

The cluster analysis resulted in four distinct cyber resilience profiles. Figure 4 visualizes the mean Z-scores of the four clusters across the seven factors, while Table 3 provides the precise values.

Table 3. Average Z-scores for the four cyber resilience clusters by factor

Cluster	Factor1	Factor2	Factor3	Factor4	Factor5	Factor6	Factor7
0	*–0.116*	*–0.854*	*–0.283*	0.108	0.228	*–0.765*	0.188
1	0.300	0.316	0.001	0.171	*–0.358*	0.439	*–0.666*
2	*–1.529*	*–0.629*	*–0.873*	*–1.505*	*–0.932*	*–0.404*	*–0.535*
3	0.565	0.604	0.651	0.527	0.690	0.299	0.829

Note: Negative factor values for individual clusters are indicated in italics.

The profiles are characterized by their unique strengths and vulnerabilities as follows:

High-risk, vulnerable individuals (Cluster 2, $N = 521$, 15.9%): This group represents the most vulnerable profile, exhibiting low cyber resilience across nearly all dimensions. They have particularly severe deficiencies in proactive data and access protection ($Z = –1.53$) and cyber threat detection ($Z = –1.51$), indicating a combined lack of technical, psychological and behavioural protective factors.

Passive problem-solvers with mental vulnerabilities (Cluster 0, N = 712, 21.7%): This group presents a paradoxical profile. While their practical skills like cyber threat detection (Z = 0.11) and online problem-solving (Z = 0.23) are average, these are overshadowed by extremely low scores in mental strength and self-control (Z = –0.85) and offline well-being (Z = –0.77). These are users who may recognize threats but lack the psychological resources to cope with stress effectively.

Cautious navigators (Cluster 1, N = 1036, 31.6%): This group displays a balanced profile characterized by a low trust in digital systems. They scored above average on proactive data protection (Z = 0.30), mental strength (Z = 0.32), and offline well-being (Z = 0.44), indicating stable internal and behavioural resources. However, their Trust in online data storage (Z = –0.67) is exceptionally low, suggesting the use of defensive online strategies.

Highly resilient, proactive, and aware individuals (Cluster 3, N = 1006, 30.7%): This group exhibits the highest level of complex cyber resilience. They perform above average on every factor, with outstandingly high scores in proactive data protection (Z = 0.57), mental strength (Z = 0.60), and trust in online data storage (Z = 0.83). This profile describes a conscious, proactive, and confident group of users with a combination of technical, psychological, and behavioural protective factors.

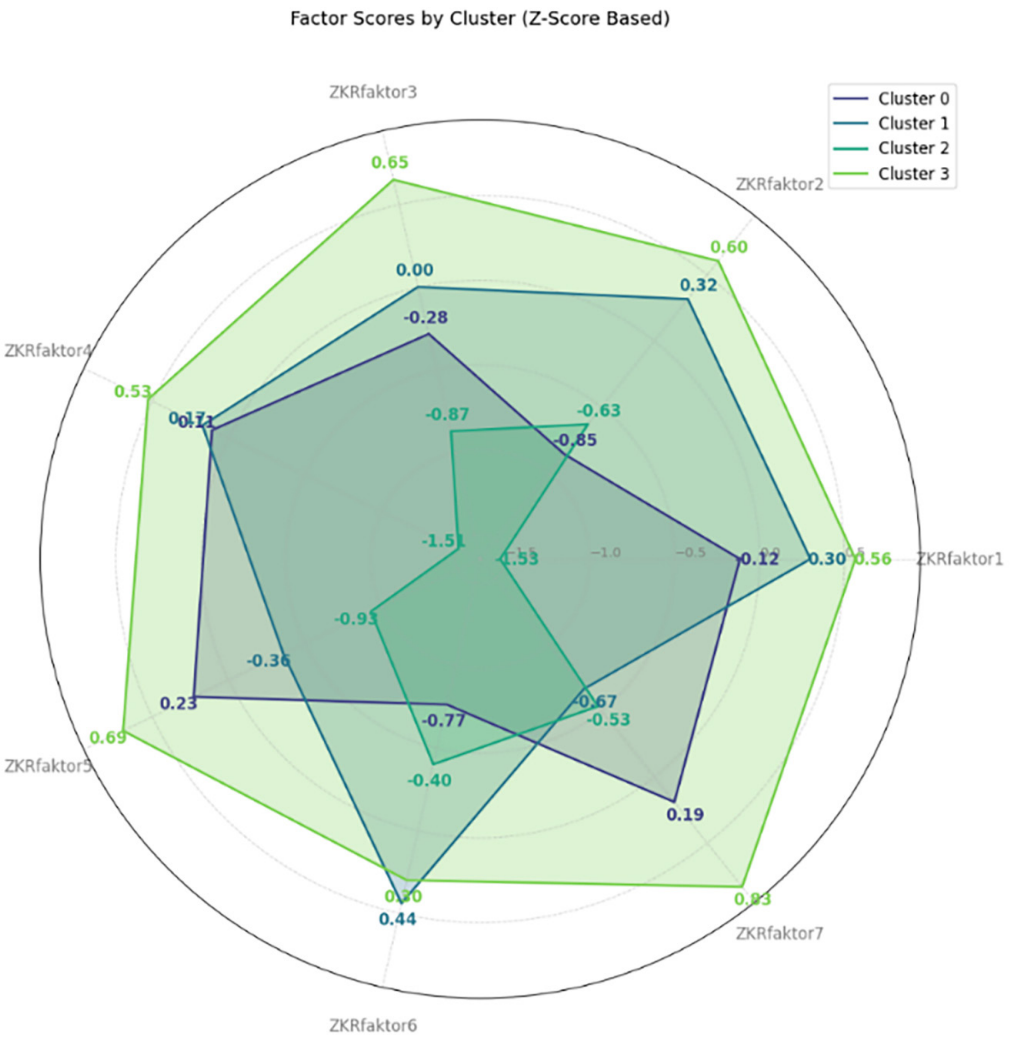

Fig. 4. Comparison of the four cyber resilience profiles along the seven factors based on average Z-scores
Source: Authors' own compilation.

4.4 Generational and gender differences in cyber resilience

An analysis of the demographic background of the cyber resilience profiles revealed significant differences for both generation and gender. A chi-square test showed that the distribution of profiles differed significantly between generations ($\chi^2(3) = 11.07$, $p = .011$) and even more markedly between genders ($\chi^2(3) = 57.64$, $p < .001$). Females were significantly overrepresented in the "Passive Problem-Solvers with Mental Vulnerabilities" cluster (Cluster 0), whereas males were overrepresented among the "Highly Resilient, Proactive, and Aware" (Cluster 3).

A more detailed investigation using a two-way analysis of variance (ANOVA) on the seven sub-dimensions further clarified these differences. Regarding gender, males scored significantly higher on mental strength and self-control ($F(1, 3271) = 49.47$, $p < .001$), active technical defence ($F(1, 3271) = 10.30$, $p = .001$), and Offline Well-being ($F(1, 3271) = 11.89$, $p < .001$). In contrast, females scored significantly higher on the Cyber Threat Detection dimension ($F(1, 3271) = 14.36$, $p < .001$). This suggests a polarization where males are stronger in internal resources and technical confidence, while females are stronger in recognizing external threats.

The main effect of generation was also significant across several factors. Members of Generation Z demonstrated higher levels of mental Strength ($p = .005$), offline well-being ($p = .007$), and online problem-solving ($p < .001$). Conversely, Generation Alpha was characterized by significantly higher Trust in Online Data Storage ($p < .001$), which may indicate a greater, possibly naiver, trust in digital systems.

An interaction effect between the two demographic variables was only marginally significant for the Mental Strength factor ($p = .063$), suggesting a trend where the gender gap in this area is more pronounced among the older Gen Z cohort.

4.5 Qualitative explanation of the profiles and differences

To gain a deeper understanding of the quantitative profiles, a thematic analysis of the focus group interviews was conducted. The analysis aimed to uncover the lived experiences, attitudes, and strategies that explain the characteristic patterns of each cluster. The following sections illustrate how the four identified profiles are reflected in the qualitative data.

The **high-risk, vulnerable** profile (Cluster 2) is characterised by a lack of specific knowledge and a resulting passive, risk-taking behaviour. Low scores on the Proactive Protection and Threat Detection factors are explained by a deficient understanding of defence strategies, as seen in responses to identifying fake websites: *"Well, I'm not good at recognising these. Neither emails nor websites like that. That's it"*. (#42_male_Z). This knowledge gap is also evident in poor password hygiene, a primary source of their vulnerability: *"I usually use the same password for everything, so I only have to remember one password"*. (#19_female_Alpha) or *"Well, I'm very careless in this respect because I have one password for everything, so if they figure that out, I'm done for ... Since I've had Facebook, for about 10 years, it's been the same."* (#47_male_Z). This lack of knowledge is coupled with a passive attitude where negative consequences, even financial loss, are normalised rather than treated as learning experiences: *"Yes, I always click on the links I receive"*. (#47_male_Z) and *"All my accounts have been hacked many times, but it doesn't bother me. Money was even spent from some of them. I lost eight thousand from one card and about 20 thousand from another"*. (#17_male_Alpha). For this group, a cycle of knowledge gaps and the normalisation of loss perpetuates their vulnerability.

The **passive problem-solvers with mental vulnerabilities** (Cluster 0) exhibit a "knowing-doing gap" high emotional reactivity, and a lack of control, which supports their paradoxical statistical profile. Members often consciously override security considerations for convenience or immediate rewards: *"Actually, if I want to download something that it won't let me because of the virus protection, I turn off the virus protection for a solid 10 minutes and download it"*. (#17_male_Alpha) or *"Usually when I'm not paying attention to security sometimes, when I'm lazy"*. (#50_male_Z). This profile is also characterized by extremely high emotional reactivity, explaining their low scores on the Mental Strength factor. Negative online interactions deeply affect them, often triggering panic or intense frustration: *"Well, something like that would affect me quite badly ... So, in these situations, I sometimes start to panic"*. (#33_female_Alpha, on receiving negative comments) or *"I lost 5 matches in a row in a game and threw my phone on the ground"*. (#32_female_Alpha). Finally, their low score on the Offline Well-being factor is linked to a diminished control over their digital behaviour, characterized by a "fear of missing out" (FOMO) and the experience of losing control: *"Well, I have that regularly. Because I simply can't stop. I just keep scrolling. The whole thing sucks you in"*. (#47_male_Z, about browsing instead of sleeping) and *"Oh my God. No. I would jump in front of a train ... that's my biggest nightmare"*. (#1_female_Alpha, on the possibility of being without internet for a few days). This profile describes a user group whose theoretical knowledge is undermined by low stress tolerance and diminished self-regulation.

The **cautious navigators** (Cluster 1) demonstrate a balanced but fundamentally distrustful profile. Their resilience stems from personal responsibility, conscious rule-following, and high emotional control. Their sense of security is based on their own proactive measures, such as using private accounts, rather than on trust in the platforms: *"From that point of view, I feel safe because on every site I'm on [...] I have a private account"*. (#19_female_Alpha) or *"Actually, I don't feel in danger, all my pages are private, so I feel less exposed to danger."* (#66_female_Z). Corresponding to their high scores on the Proactive Protection factor, this group applies specific, rule-based defence strategies. They use modern security tools and respond to threats with automatic, ingrained reactions: *"For me, it's two-step authentication on online platforms, password and fingerprint on my phone"*. (#58_male_Z), *"I block it immediately and don't click on it, so I ignore it"*. (#49_male_Z, on suspicious links), and *"Well, I think the font style, grammar and if they really want you to download something and are rushing you"*. (#18_male_Alpha, on identifying fake websites). Their high score on the Mental Strength factor is explained by their calm, rational responses to negative online interactions. Instead of overreacting emotionally, they are able to assess the situation objectively and maintain emotional distance, treating criticism as the other person's opinion rather than an attack on their self-worth: *"If I get it from a stranger, then I don't deal with it."* (#3_female_Alpha) and *"Well, if they say something negative, honestly, I'm not usually interested in other people's negative opinions. I mean, okay, they have an opinion about me, but that's theirs. I'm not going to get offended by it"*. (#21_female_Alpha). This cluster is a conscious, prepared group whose resilience is based on a healthy scepticism of the digital environment and strong internal psychological and behavioural control.

The **highly resilient, proactive, and aware** (Cluster 3) profile emerges in the qualitative data as a proactive, learning-oriented, and emotionally balanced group. They not only know but also confidently and consistently apply modern defence strategies. For them, security is not a burden but an internalized, automatic habit, and they are able to identify threats based on subtle cues: *"I use a strong password. It has many characters ... I also use two-step authentication or an authenticator key,*

and a VPN". (#84_male_Z). Instead of becoming passive victims or reacting impulsively, they view experiences as opportunities for personal growth and conscious emotional regulation: *"I was bullied a lot when I was younger ... Fortunately, I've learned to handle it now, so if someone says a bad word about me, I just let it go and move on*". (#57_male_Z) or *"I've grown out of that now, I try to handle problems calmly now, for example, if I can't connect to the Wi-Fi immediately, I take a deep breath and then I start trying again. I've learned to control my temper*". (#57_male_Z). For them, the internet is a tool, not the centre of their lives. They view the possibility of being offline not with anxiety, but as an opportunity for real-world alternatives: *"I would be happy about it. Because then at least people wouldn't be calling me and I would have more time for things I would do otherwise*". (#5_female_Alpha) and *"It wouldn't bother me that much, there have been regular times when I haven't used my phone for several days because I didn't need to*". (#76_female_Z). This group has successfully integrated technical knowledge, psychological resources, and conscious behavioural strategies. They are able to use the digital space confidently and securely while maintaining control over their online presence and protecting their mental well-being.

5 DISCUSSION

This study pursued two primary objectives: to develop a new instrument for measuring youth cyber resilience, the PCRS, and to use this tool to identify typical user profiles and demographic differences. Our results confirm and empirically support the emerging theoretical framework that cyber resilience is not a monolithic capability but a multidimensional, complex construct [5], [6]. The seven distinct yet correlated factors of the PCRS, ranging from proactive behaviours and psychological coping to technical knowledge, accurately reflect this multifaceted nature.

The study's most significant theoretical contribution is the identification of four statistically and qualitatively validated cyber resilience profiles. These profiles move beyond a simple "resilient vs. non-resilient" dichotomy to offer a more nuanced typology. While the "Highly Resilient" and "High-Risk" profiles represent the two ends of the spectrum, the intermediate groups, particularly the paradoxical "Passive Problem-Solvers with Mental Vulnerabilities", highlight a key theoretical insight. The existence of this group illuminates the critical "knowing-doing gap" in the digital space [10], [27]. Qualitative data clearly showed that these participants often possess the knowledge to recognise risks but are unable to translate this knowledge into effective protective behaviour's. This finding indicates that cybersecurity knowledge and technical skills alone are insufficient for genuine cyber resilience; psychological resources such as stress tolerance, emotional regulation, and self-regulation skills are at least as important, if not more so [4], [5], [6], [10].

The demographic analyses further enrich this picture, revealing that gender and generational affiliation systematically influence these profiles. The findings, such as the over-representation of females in the more mentally vulnerable group [4], [16] or the higher online trust of the Alpha generation [20], align with existing literature that emphasises the different digital socialisation paths and risk exposures between genders and generations [4], [9], [10], [16], [20], [28].

The PCRS can serve as a diagnostic tool in education to identify at-risk groups. The identified profiles enable a move beyond a "one-size-fits-all" approach, allowing for the development of targeted, differentiated interventions. While the "High-Risk" group requires fundamental knowledge and skill development, the "Passive Problem-Solvers" would benefit more from programmes focused on mental health, stress management, and self-regulation.

This study has limitations, including its sample being confined to a single Hungarian county, which reduces generalisability, and its cross-sectional data, which precludes causal inferences. Future longitudinal studies are needed to examine the temporal stability of these profiles and the familial and school-related factors underlying their development. Further validation of the PCRS on international samples and the revision of one item with a low factor loading are also warranted to strengthen the factor's internal consistency.

In conclusion, our study provides researchers and practitioners with a new, reliable tool for measuring youth cyber resilience. Through the identified profiles, it offers deeper insight into the heterogeneity of online coping strategies among digital natives.

6 CONCLUSION

This study successfully developed and validated the PCRS, a multidimensional instrument capable of capturing the complexity of young people's online coping capabilities. Through the application of this scale, our research moves beyond the homogeneous view of "digital natives" by revealing four distinct cyber resilience profiles that demonstrate varied patterns of vulnerability and strength. The identification of these profiles—particularly the "Passive Problem-Solvers with Mental Vulnerabilities"—underscores that cyber resilience is not merely a matter of technical skill but is deeply intertwined with psychological resources and self-regulation.

The discovery of significant generational and gender differences across these profiles provides a crucial empirical foundation for moving beyond generic digital literacy programmes. Instead, our findings advocate for the development of targeted, data-driven interventions that address the specific needs of different user groups. Such strategies would involve foundational skill-building for the "High-Risk" profile, while focusing on mental health and stress management support for the "Passive Problem-Solvers".

In conclusion, this study offers a robust methodological tool and a nuanced empirical framework for both researchers and practitioners. It provides a deeper understanding of the heterogeneity of online coping strategies and equips stakeholders with the means to better comprehend and more effectively support the digital well-being of the youngest generations in an increasingly complex online world.

7 REFERENCES

[1] Z. Deák, J. T. Karlovitz, and J. Kárpáti-Daróczi, "Digital communication patterns in families: Generational and country of origin effects," *Acta Polytechnica Hungarica*, vol. 21, no. 8, pp. 309–329, 2024. https://doi.org/10.12700/APH.21.8.2024.8.16

[2] R. Subashini, "Transformative approach in engineering curricula: Enhancing computational thinking through literacy skills for engineering learners," *International Journal of Engineering Pedagogy (iJEP)*, vol. 15, no. 5, pp. 141–149, 2025. https://doi.org/10.3991/ijep.v15i5.53461

[3] M. Serik, D. Tleumagambetova, S. Tutkyshbayeva, and A. Zakirova, "Integration of cybersecurity into computer science teachers' training: A systematic review," *International Journal of Engineering Pedagogy (iJEP)*, vol. 15, no. 4, pp. 57–75, 2025. https://doi.org/10.3991/ijep.v15i4.53127

[4] M. Adorjan and R. Ricciardelli, *Cyber-Risk and Youth, Digital Citizenship, Privacy, and Surveillance*. London: Routledge, 2018. https://doi.org/10.4324/9781315158686

[5] H. Sun, C. Yuan, Q. Qian, S. He, and Q. Luo, "Digital resilience among individuals in school education settings: A concept analysis based on a scoping review," *Frontiers in Psychiatry*, vol. 13, p. 858515, 2022. https://doi.org/10.3389/fpsyt.2022.858515

[6] R. S. Qamaria, D. Kuswandi, N. Setiyowati, and A. M. Bahodirovna, "Digital resilience in adolescence: A systematic review of models, methods and theoretical perspectives," *Multidisciplinary Reviews*, vol. 8, no. 9, p. 2025287, 2025. https://doi.org/10.31893/multirev.2025287

[7] R. Sell, R. Razdan, K. Kase, and T. Rüütmann, "The role of AI chatbots in engineering education: Experimental findings and implementation strategies," *International Journal of Engineering Pedagogy (iJEP)*, vol. 15, no. 5, pp. 4–19, 2025. https://doi.org/10.3991/ijep.v15i5.56681

[8] L. Bognár and L. Bottyán, "Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students," *Education Sciences*, vol. 14, no. 6, p. 588, 2024. https://doi.org/10.3390/educsci14060588

[9] I. Arpaci and K. Sevinc, "Development of the cybersecurity scale (CS-S): Evidence of validity and reliability," *Information Development*, vol. 38, no. 2, pp. 218–226, 2021. https://doi.org/10.1177/0266666921997512

[10] J. T. Módné and M. Pogátsnik, "A comprehensive study on cybersecurity awareness: Adaptation and validation of a questionnaire in Hungarian Higher Technical education," *Acta Polytechnica Hungarica*, vol. 21, no. 10, pp. 533–552, 2024. https://doi.org/10.12700/APH.21.10.2024.10.32

[11] I. Arpaci, O. Aslan, and I. E. Oner, "Cybersecurity Awareness Scale (CSAS) for social media users: Development, validity and reliability study," *Information Development*, 2025. https://doi.org/10.1177/02666669251336562

[12] R. Járai, D. Vajda, R. Hargitai, L. Nagy, K. Csókási, and E. C. Kiss, "A Connor–Davidson Reziliencia kérdőív 10 itemes változatának jellemzői [The Connor–Davidson Resilience Scale: Psychometric properties of the 10-item version]," *Alkalmazott Pszichológia* [*Applied Psychology*], vol. 15, no. 1, pp. 129–136, 2015. https://doi.org/10.17627/ALKPSZICH.2015.1.129. [in Hungarian].

[13] H. Jonkman, M. van Rooijen, M. Wiersma, and R. van Goor, "Validation study of the Child and Youth Resilience Measure (CYRM-28) among Dutch youth," *Frontiers in Psychiatry*, vol. 13, p. 637760, 2022. https://doi.org/10.3389/fpsyt.2022.637760

[14] Eurostat – Statistics Explained, "Young people – digital world," 2025. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world

[15] M. Anderson, M. Faverio, and J. Gottfried, "Teens, social media and technology 2023," Pew Research Center, 2023. [Online]. Available: https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023

[16] V. Stavropoulos, F. Motti-Stefanidi, and M. D. Griffiths, "Risks and opportunities for youth in the digital era: A cyber-developmental approach to mental health," *European Psychologist*, vol. 27, no. 2, pp. 86–101, 2021. https://doi.org/10.1027/1016-9040/a000451

[17] V. Pérez-Torres, "Social media: A digital social mirror for identity development during adolescence," *Current Psychology*, vol. 43, pp. 22170–22180, 2024. https://doi.org/10.1007/s12144-024-05980-z

[18] The Annie E. Casey Foundation, "The impact of social media and technology on gen alpha," 2025. [Online]. Available: https://www.aecf.org/blog/impact-of-social-media-on-gen-alpha

[19] Sutresna, "Decoding generation alpha: How the youngest digital natives use, think, and choose," Medium, 2025. [Online]. Available: https://dsutresna.medium.com/decoding-generation-alpha-how-the-youngest-digital-natives-use-think-and-choose-b8ab81047259

[20] A. Höfrová, V. Balidemaj, and M. A. Small, "A systematic literature review of education for Generation Alpha," *Discover Education*, vol. 3, p. 125, 2024. https://doi.org/10.1007/s44217-024-00218-3
[21] W. Janssens, K. Wijnen, P. de Pelsmacker, and P. Van Kenhove, *Marketing Research with SPSS*. New York, NY: FT Publishing International, 2010.
[22] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951. https://doi.org/10.1007/BF02310555
[23] S. Carpenter, "Ten steps in scale development and reporting: A guide for researchers," *Communication Methods and Measures*, vol. 12, no. 1, pp. 25–44, 2018. https://doi.org/10.1080/19312458.2017.1396583
[24] D. Hooper, J. Coughlan, and M. Mullen, "Structural equation modelling: Guidelines for determining model fit," *Electronic Journal of Business Research Methods*, vol. 6, no. 1, pp. 53–60, 2008.
[25] L. Sajtos and A. Mitev, *SPSS kutatási és adatelemzési kézikönyv* [*SPSS Research and Data Analysis Manual*]. Budapest: Alinea Kiadó, 2007. [in Hungarian].
[26] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006. https://doi.org/10.1191/1478088706qp063oa
[27] A. Tick and T. M. Phuong, "Cyber security awareness and the behaviors of higher education students using smartphones in Vietnam," *Acta Polytechnica Hungarica*, vol. 21, no. 12, pp. 111–131, 2024. https://doi.org/10.12700/APH.21.12.2024.12.7
[28] C. Qi and N. Yang, "Digital resilience in Chinese adolescents: A portrayal of the current condition, influencing factors, and improvement strategies," *Frontiers in Psychiatry*, vol. 15, p. 1278321, 2024. https://doi.org/10.3389/fpsyt.2024.1278321

8 AUTHORS

Judit Módné Takács is an assistant professor and deputy head of institute at the Alba Regia Faculty of Obuda University, Székesfehérvár, Hungary. Her research focuses on engineering education, cybersecurity awareness, the development of soft skills in technical training, adult education methodologies, and innovative approaches that motivate students to engage with and apply STEM subjects in practice (E-mail: modne.t.judit@amk.uni-obuda.hu).

Monika Pogátsnik is an associate professor and vice dean for education at the Alba Regia Faculty of Obuda University. Her main research area is engineering pedagogy, with a special emphasis on work-based learning, non-cognitive skills, and career attitudes (E-mail: pogatsnik.monika@amk.uni-obuda.hu).