Digital Transformation in Higher Education Obstacle Assessment and Development of Strategies against Cybersecurity Threats: The Case of Moroccan Universities

Abdelilah Chahid
Higher Normal School of Technical Education, Casablanca, Morocco
chahidabdelillah@gmail.com (corresponding author)

Souad Ahriz
Higher Normal School of Technical Education, Casablanca, Morocco
ahrizsouad@gmail.com

Kamal El Guemmat
Higher Normal School of Technical Education, Casablanca, Morocco
k.elguemmat@gmail.com

Khalifa Mansouri
Higher Normal School of Technical Education, Casablanca, Morocco
khalifa.mansouri@enset-media.ac.ma

Received: 29 August 2024 | Revised: 25 September 2024, 20 October 2024, and 26 October 2024 | Accepted: 7 December 2024

 DOI: https://doi.org/10.48084/etasr.8853

ABSTRACT

Digital Transformation(DT) in higher education has become essential in improving both educational delivery and operational efficiency. However, this transition also exposes institutions to increasing cybersecurity threats, often associated with various barriers reported in the literature. Although these barriers have been widely studied, no research has yet systematically prioritized them in the academic context. This study, conducted within the framework of DT in Morocco, addresses this gap by classifying and prioritizing these barriers to better understand how they contribute to the spread of cybersecurity threats. Using methodologies such as the Analytic Hierarchy Process (AHP) and the Analytic Network Process (ANP), we not only prioritized the major barriers but also developed specific strategies to counter the resulting threats, revealing significant variations in the prioritization of cybersecurity strategies. These differences arise from the complex interactions between the barriers identified by the ANP, highlighting the importance of considering interdependencies when developing effective cybersecurity strategies.

Keywords-cybersecurity; AHP; ANP; digital transformation

I. INTRODUCTION

Digital Transformation (DT) has become a central pillar of economic and social development in the modern world. It is widely recognized for its ability to stimulate innovation and redefine business models across various sectors, including education [1]. DT is no longer just a response to technological advancements but has become a necessity for businesses and institutions seeking to maintain their competitiveness and avoid obsolescence [2]. Numerous studies have explored the optimization of digital transformation, viewing it as a crucial lever for change and adaptation in an increasingly digitized global environment [3]. However, the diversity of definitions and approaches to DT complicates its analysis and implementation [4]. In this context, organizations and governments acknowledge the need for quick and effective adaptation to remain competitive in an ever-evolving market [5]. In the higher education sector, DT leads to profound changes in teaching practices, infrastructure, curricula, administration, human resource management, and information governance [6]. The COVID-19 pandemic accelerated this transformation, forcing institutions to rapidly adopt distance learning methods while taking into account the diversity of their structures [7]. Morocco, through the Morocco Digital

2020 initiative, has embarked on the digitization of its universities [8]. However, the country ranks 77th globally according to the Global Innovation Index 2021 [9], revealing the complexity of this transition, exacerbated by numerous obstacles that also increase vulnerabilities to cybersecurity threats. To address this gap, this study aims to classify and prioritize the obstacles to DT in Moroccan universities, considering their impact on the spread of cybersecurity threats. To do so, multi-criteria analysis methods, such as the Analytic Hierarchy Process (AHP) and the Analytic Network Process (ANP), were used. These approaches help evaluate the relative importance of each obstacle and identify specific strategies to counter the associated threats.

II. OBSTACLES TO DIGITAL TRANSFORMATION IN HIGHER EDUCATION

DT in higher education faces numerous obstacles [10-13], including strategic, technological, and organizational challenges, which not only slow down the transformation process but also increase vulnerabilities related to cybersecurity. Institutions face deficits in strategic planning and the absence of a clearly defined vision, along with governance issues and inadequate policies. On the technological front, the integration of IT in higher education is hampered by insufficient infrastructure and inadequate support services. Additionally, the lack of digital skills combined with organizational and cultural resistance to change, prevents the effective adoption of digital technologies. Economic and budgetary constraints further limit institutions' ability to invest in the tools and infrastructure needed for digital transformation. These interconnected obstacles slow down the DT of higher education institutions while exacerbating cybersecurity risks. Table I presents the main obstacles to DT in higher education institutions, grouped into five categories.

III. CYBERSECURITY THREATS AND RISKS ASSOCIATED WITH DIGITAL TRANSFORMATION IN UNIVERSITIES

Cybersecurity threats are a major obstacle to the progress of DT in universities. Cybercrime, in particular, is seen as one of the most significant challenges in this area [14-18]. Cyberattacks, especially those sponsored by states, often target the critical infrastructure weaknesses of institutions [19]. Moreover, the vulnerability to opportunistic attackers is heightened due to the lack of robust security protocols [20]. The management of internal threats, such as attacks initiated by organization members or human errors, is also a challenge. Developing efficient automated systems to monitor and analyze these threats remains a complex task [21]. Table II summarizes the main cybersecurity threats in HEIs during their digital transformation, grouped in five categories.

TABLE I. BARRIERS AND SUB-BARRIERS TO DT

Category of Barriers	References	Sous Barriers
Strategic (S)	[22-25]	Deficiency in strategic planning (S1)
	[22, 23, 26]	Absence of a defined vision (S2)
	[27-30]	Governmental vision, planning, and policies (S3)
	[26, 31, 22]	Inadequate implementation planning, time constraints, competing priorities (S4)
Technological (T)	[22, 23, 32]	Challenges in integrating IT into higher education (T1)
	[6, 22, 23]	IT security risks (T2)
	[3, 22, 23]	Inadequate IT infrastructure (T3)
	[6, 34, 35]	Unsuitable IT infrastructure and support services (T4)
Skills and Human Resources (SHR)	[22, 23, 33]	Lack of pedagogical expertise and experience (SHR1)
	[7, 26, 31, 36]	low level of digital literacy(SHR2)
	[32, 35, 37]	Lack of human resources (SHR3)
	[38-41]	Leadership skills and behavior (SHR4)
Organizational and cultural barriers (O)	[42-44]	Lack of coordination between departments (O1)
	[22, 23, 45]	Human resistance to change (O2)
	[22-24]	Shortfall in innovation (O3)
Environmental (E)	[22, 23, 26]	Economic climate (E1)
	[27-29, 46]	Budgetary limitation (E2)

TABLE II. THREATS TO DIGITAL TRANSFORMATION IN HEIS

Threat	Intention	Threat Events	References
Cybercrime (CY)	Unauthorized access, online fraud, identity theft	Malware, phishing, exploitation of security vulnerabilities, denial-of-service (DDoS) attacks, and identity theft	[47, 48]
State-Sponsored Espionage (ES)	Unauthorized access, data collection, acquisition of classified information	Advanced cyber espionage, targeted attacks, long-term network infiltration	[47, 49]
Human Errors (EH)	Unintentional errors due to negligence or lack of knowledge	Accidental sharing of sensitive information, incorrect system configurations, non-compliance with security policies, and poor access management	[50, 51]
Opportunists	Exploiting favorable circumstances or obvious vulnerabilities without prior planning	Vulnerability scans, opportunistic attacks, and exploitation of crisis situations	[51]
Insider (IN)	Acting against the interests of an organization for personal gain, revenge, ideology, or under third-party coercion	Data theft or sabotage, unauthorized access to sensitive information, and manipulation of internal systems	[52-54]

IV. METHOD AND DATA COLLECTION

A. The ANP and AHP Approaches

ANP is defined as a multi-criteria theory of measurement used to derive relative priority scales of absolute numbers from individual judgments (or from actual measurements normalized to a relative form) that also belong to a fundamental scale of absolute numbers [55]. Similarly, AHP is defined as a systematic approach for problems that include the thought of different criteria in a hierarchical model. AHP reflects human thinking by grouping the elements of a problem requiring complex and multi-aspect decisions [56]. Both concepts were developed in [57] as means of finding an effective and powerful methodology that can deal with complex decision-making problems. In the ANP method, dependencies among various criteria are considered differentiating it from the AHP. The ANP uses a network without the need to specify levels. Dominance or the relative importance of influence is a central concept in, AHP. A judgment is formed from the fundamental scale of the AHP by answering two questions: (a) Given a criterion, which of the two elements is more dominant with respect to that criterion, (b) which of the two elements influences a third element more, with respect to a criterion [58]? In pairwise comparisons, entered values mirror the relative effect among elements with respect to a control criterion. These entered values are based on the importance of each criterion. The network structure consists of different clusters, and these clusters contain various nodes or elements.These clusters are connected to each other based on the relative influences among the nodes. Authors in [59] developed a numerical scale for assigning the weight for criteria or alternative by giving a value between 1 (equal importance) and 9 (extreme importance).

B. Data Collection

As noted in [60], the AHP and the ANP do not require large samples as they are not statistical methods. In fact, authors in [61] emphasize that these approaches focus on the analysis of decisions rather than the characteristics of the individuals making them. For this study, the data for the pairwise comparisons of factors were collected from 32 business and IT managers from various higher education institutions (HEIs) in Morocco, following the methodology of [62]. A convenience sampling method was used, with respondents selected based on their key roles in managing digital transformation and cybersecurity within their institutions. The sample consisted of 35% business managers and 65% IT managers, a distribution justified by their respective expertise in these areas. The data were collected through a questionnaire based on pairwise comparisons, allowing for the prioritization of obstacles to digital transformation. The first phase of the study identified five main categories of obstacles and 17 sub-obstacles, drawn from a detailed literature review (see Tables I and II). Based on these sub-obstacles, five cybersecurity strategies specific to the associated threats were developed by experts, relying on the results of pairwise comparisons. These strategies, presented in Table III, were designed to mitigate vulnerabilities related to DT in higher education institutions. It is noted that experts emphasize the importance of solid cybersecurity training for every strategy, which demonstrates that such training plays a crucial role in improving security practices within institutions by addressing human vulnerabilities, a point widely supported by the literature. Authors in [63] demonstrated that the DeapSECURE program at ODU, effectively bridges the gaps in traditional cybersecurity programs by exposing students to real-world challenges. Additionally, authors in [64] highlight that well-structured training programs significantly influence user behavior, thereby reducing human vulnerabilities. It has also been shown that increasing training hours is directly correlated with a reduction in cyber incidents [65]. Lastly, pedagogical approaches based on gamification, such as the GenCyber program at Purdue University, enhance student engagement and their cybersecurity skills [66]. The analytical network model used in this research is illustrated in Figure 1.

TABLE III. THREAT CATEGORIES AND SUGGESTED STRATIES

Threat Type	Strategies
Cybercrime (CY)	SCY (Advanced security infrastructure, Cybersecurity training programs, Automatic update policies, Regular backups and recovery tests, Incident response plan)
State Espionage (ES)	SES (Research risk assessment, Enhanced access control, Partnerships with government agencies, Secure communications, Regular security audits, Sensitive Information Security Training)
Human Errors (EH)	SEH (Clear policies and procedures, Ongoing awareness and training, Identity access management, Accessible technical support, Periodic security practice reviews)
Opportunists (OP)	SOP (Training on physical security and network access protection,Physical security of buildings, Securing Wi-Fi networks, Strict password policies, Proactive network monitoring, Regular penetration tests)
Internal Risks (IN)	SIN (Specific training on internal risks, Monitoring risky behaviors, Access rights management, Privacy policies, Anonymous reporting channels)

V. RESULTS AND DISCUSSION

Table IV shows that the highest priorities among the sub-factors belong to SHR2 (0.545), followed by S1 (0.325), and finally T1, (0.196). The main obstacles to DT in higher education are related to human skills, strategy, and technology. A clear strategy, robust technological infrastructure, and a high level of digital literacy are essential. Although organizational and cultural barriers are less critical, they remain important, as do environmental and budgetary constraints, even if these seem to be less urgent challenges. Our study stands out with its rigorous quantitative methodology, which prioritizes the obstacles in a precise manner, unlike the qualitative approaches of other studies. For instance, [67] provides an in-depth analysis of strategic and organizational obstacles, but without measurable prioritization, while [11] proposes a systematic framework based on expert validation. Studies [68] and [69] focus respectively on inclusivity and the balance between skills and innovation,offering complementary perspectives, while [70] emphasizes the importance of digital culture and transformational leadership.

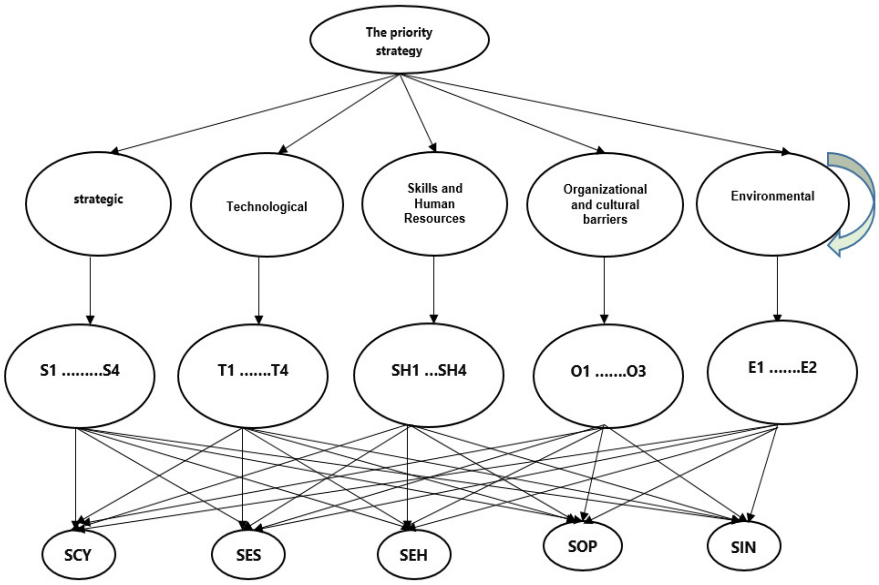

Fig. 1. ANP model for barriers.

Cybersecurity is an aspect often neglected in previous studies [11, 32, 42, 43, 71, 72]. Table V presents an analysis of cybersecurity strategies identified in the literature on DT. For example, authors in [73] emphasize in the importance of strategies aimed at managing cyberattacks by focusing on sustainable management practices and authors in [15] recommend the use of advanced technologies such as blockchain and quantum computing to mitigate threats such as ransomware and identity theft. Authors in [74] stress the need for continuous training and awareness of human risks, while authors in [75] highlight the importance of developing practical skills to support DT. These studies provide an overview of existing strategies, but they do not explicitly prioritize different types of threats or internal interactions that may exacerbate these risks. In contrast, Table VI presents the results of our own analysis using multi-criteria methods such as AHP and ANP to prioritize cybersecurity strategies in a specific context. Although the most critical strategies, such as SCY and SE, and the least critical, SEH, retain the same order as in AHP, a change is observed between the SOP and SIN strategies. With ANP, SIN moves from the fourth to the third place, while SOP drops by one position. This change is explained by the interactions between sub-obstacles, which give more weight to the behaviors and activities of internal actors within universities. For instance, a sub-obstacle like the low level of digital literacy (SHR2) may exacerbate IT security risks (T2), thereby increasing vulnerabilities and the risk of internal attacks. Unlike the strategies from the literature presented in Table V, our analysis, illustrated in Table VI, integrates these internal interactions and prioritizes threats more precisely. Thus, our work makes a unique contribution by providing a measurable prioritization of cybersecurity strategies, allowing higher education institutions to better prepare for specific threats, such as internal and opportunistic risks, which are often underestimated in the strategies identified in the literature.

TABLE IV. OVERALL PRIORITY OF THE BARRIER SUB-FACTORS

Barrier factors	Factor priority	Barrier sub-factors	Sub-factor priority	Overall sub-facto priority	Rank
Strategic (S)	0.596	Lack of strategy (S1)	0.546	0.325	2
		Lack of clear vision (S2)	0.232	0.138	4
		Government vision, plan, and policy (S3)	0.083	0.049	14
		Lack of implementation action plan, lack of time, and other priorities (S4)	0.137	0.081	9
Technological (T)	0.406	Difficulties embedding IT into higher education (T1)	0.484	0.196	3
		IT security risks (T2)	0.260	0.105	8
		Lack of adequate IT infrastructure (T3)	0.096	0.038	17
		Unsuitable IIT infrastructure and support services (T4)	0.159	0.064	13
Skills and Human Resources (SHR)	0.545	Lack of pedagogical skills and experience (SHR1)	0.232	0.126	7
		The low level of the digital literacy (SHR2)	0.546	0.545	1
		Lack of human resources (SHR3)	0.137	0.074	10
		Leadership skills and behavior (SHR4)	0.083	0.045	15
Organizational and cultural barriers (O)	0.248	Lack of coordination between departments (O1)	0.163	0.040	16
		Human resistance to change (O2)	0.539	0.133	5
		Lack of innovation(O3)	0.296	0.073	11
Environmental(E)	0.197	Economic environment (E1)	0.666	0.131	6
		Budgetary constraints(E2)	0.333	0.065	12

TABLE V. ANALYSIS OF CYBERSECURITY STRATEGIES IN DIGITAL TRANSFORMATION STUDIES

Ref.	Main Strategies	Methodology	Strategy Prioritization
[72]	-Cybersecurity strategies -Cyberattack management	Cyber risk analysis	Emphasizes the importance of cybersecurity to counter cyberattacks during digital transformation.
[15]	-Use of advanced technologies (blockchain, quantum computing) -Protection against ransomware	Cybersecurity -based approach	Recommends advanced technologies to mitigate threats, particularly against ransomware and identity theft.
[73]	-Cybersecurity training -Human risk awareness	Training and awareness	Highlights the importance of training and awareness to minimize human risks, aligned with SEH and SIN.
[74]	-Development of cybersecurity skills to support digital transformation	Study of European initiatives	Supports the importance of developing practical cybersecurity skills to better protect digital infrastructures.

TABLE VI. STRATEGY WEIGHTINGS AND RANKINGS

Weighting and ranking strategies with AHP and ANP					
	SCY	SES	SEH	SOP	SIN
Weights in AHP	0.372	0.280	0.082	0.141	0.117
Ranking in AHP	1	2	5	3	4
Weights in ANP	0.880	0.628	0.186	0.257	0.270
Ranking in ANP	1	2	5	4	3

VI. CONCLUSION

The current study makes a significant contribution to the understanding of the barriers to Digital Transformation (DT) in higher education, particularly regarding their impact on cybersecurity threats. By using multi-criteria analysis methods such as AHP and ANP, we were able not only to classify and prioritize these barriers but also to develop specific cybersecurity strategies to counter the associated threats. One of our main contributions is the recognition of the importance of interconnections between sub-barriers and their influence on institutional vulnerabilities, which allowed us to propose more effective cybersecurity strategies tailored to the realities of higher education institutions.

However, this work has some limitations. Firstly, the sample used for pairwise comparisons is relatively small (32 experts), which may limit the generalization of the results. Secondly, the study focused on Moroccan universities, and while the findings may be relevant internationally, they might need to be adapted to different cultural and economic contexts. Finally, we did not exhaustively explore certain dimensions such as the long-term psychosocial impacts of cyberattacks on staff and students, a crucial aspect that deserves more in-depth analysis in future research. Despite these limitations, our research opens promising perspectives for better management of cybersecurity risks in the digital transformation of universities.

REFERENCES

[1] A. Kozarkiewicz, "General and Specific: The Impact of Digital Transformation on Project Processes and Management Methods," *Foundations of Management*, vol. 12, no. 1, pp. 237–248, 2020, https://doi.org/10.2478/fman-2020-0018.

[2] T. M. Siebel, *Digital Transformation: Survive and Thrive in an Era of Mass Extinction*. New York, NY, USA: RosettaBooks, 2019.

[3] Y. Yoo, R. J. Boland, K. Lyytinen, and A. Majchrzak, "Organizing for Innovation in the Digitized World," *Organization Science*, vol. 23, no. 5, pp. 1398–1408, 2012, https://doi.org/10.1287/orsc.1120.0771.

[4] J. Reis, M. Amorim, N. Melao, and P. Matos, "Digital Transformation: A Literature Review and Guidelines for Future Research," in *World Conference on Information Systems and Technologies*, Galicia, Spain, Apr. 2019, pp. 411–421, https://doi.org/10.1007/978-3-319-77703-0_41.

[5] J. S. Morrison, "Organizational Change for Corporate Sustainability-A Guide for Leaders and Change Agents of the Future," *Journal of Education for Business*, vol. 79, no. 2, pp. 124–125, 2003.

[6] L. M. C. Benavides, J. A. Tamayo Arias, M. D. Arango Serna, J. W. Branch Bedoya, and D. Burgos, "Digital Transformation in Higher Education Institutions: A Systematic Literature Review," *Sensors*, vol. 20, no. 11, Jan. 2020, Art. no. 3291, https://doi.org/10.3390/s20113291.

[7] T. Jensen, *Higher Education in the Digital Era*. IAU, 2019.

[8] D. Ferhane and L. Yassine, "La transformation numerique de l'universite marocaine a l'epreuve de la covid 19: transition vers un modele universitaire agile," *International Journal of Trade and Management*, vol. 1, no. 1, pp. 55–69, May 2022, https://doi.org/10.34874/PRSM.ijtm-vol1iss1.97.

[9] H. Tamer and Z. Knidiri, "University 4.0: Digital Transformation of Higher Education Evolution and Stakes in Morocco," *American Journal of Smart Technology and Solutions*, vol. 2, no. 1, pp. 20–28, Mar. 2023, https://doi.org/10.54536/ajsts.v2i1.1300.

[10] I. Nurhas, B. R. Aditya, D. W. Jacob, and J. M. Pawlowski, "Understanding the challenges of rapid digital transformation: the case of COVID-19 pandemic in higher education," *Behaviour and Information Technology*, vol. 41, no. 13, pp. 2924–2940, Oct. 2022, https://doi.org/10.1080/0144929X.2021.1962977.

[11] B. R. Aditya, R. Ferdiana, and S. S. Kusumawardani, "A barrier diagnostic framework in process of digital transformation in higher education institutions," *Journal of Applied Research in Higher Education*, vol. 14, no. 2, pp. 749–761, Jul. 2021, https://doi.org/10.1108/JARHE-12-2020-0454.

[12] V. J. Garcia-Morales, A. Garrido-Moreno, and R. Martin-Rojas, "The Transformation of Higher Education After the COVID Disruption: Emerging Challenges in an Online Learning Scenario," *Frontiers in Psychology*, vol. 12, Feb. 2021, https://doi.org/10.3389/fpsyg.2021.616059.

[13] M. Laufer *et al.*, "Digital higher education: a divider or bridge builder? Leadership perspectives on edtech in a COVID-19 reality," *International Journal of Educational Technology in Higher Education*, vol. 18, no. 1, Sep. 2021, Art. no. 51, https://doi.org/10.1186/s41239-021-00287-6.

[14] C. L. Kendall, "The Openness of Higher Education and Implications on Cybersecurity," M.S. thesis, Utica University, Utica, NY, USA, 2022.

[15] K. Sandhu, "Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges," in *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, Hershey, PA, USA: IGI Global, 2021, pp. 1–17.

[16] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, Jan. 2023, Art. no. 6666, https://doi.org/10.3390/s23156666.

[17] E. Pavlova, "Enhancing the Organisational Culture related to Cyber Security during the University Digital Transformation," *Information & Security: An International Journal*, vol. 46, no. 3, pp. 239–249, 2020, https://doi.org/10.11610/isij.4617.

[18] H. Taherdoost, M. Madanchian, and M. Ebrahimi, "Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges," in *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, Hershey, PA, USA: IGI Global, 2021, pp. 99–117.

[19] H. Durojaye and O. Raji, "Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure." arXiv, Dec. 13, 2022, https://doi.org/10.48550/arXiv.2212.08036.

[20] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity Risks in a Pandemic," *Journal of Medical Internet Research*, vol. 22, no. 9, Sep. 2020, Art. no. e23692, https://doi.org/10.2196/23692.

[21] D. Chitre, A. Dhoke, and A. Shriniwar, "A Review: Insider Attack in New Normal," *International Journal of Scientific Research in Engineering and Management*, vol. 6, no. 6, pp. 1–14, Jun. 2022, https://doi.org/10.55041/IJSREM16118.

[22] A. Marks and M. AL-Ali, "Digital Transformation in Higher Education: A Framework for Maturity Assessment," in *COVID-19 Challenges to University Information Technology Governance*, M. Alaali, Ed. Springer, 2022, pp. 61–81.

[23] M. AL-Ali and A. Marks, "A Digital Maturity Model for the Education Enterprise," *Perspectives: Policy and Practice in Higher Education*, vol. 26, no. 2, pp. 47–58, 2022, https://doi.org/10.1080/13603108.2021.1978578.

[24] M. A. Mohamed Hashim, I. Tlemsani, and R. Duncan Matthews, "A sustainable University: Digital Transformation and Beyond," *Education and Information Technologies*, vol. 27, no. 7, pp. 8961–8996, Aug. 2022, https://doi.org/10.1007/s10639-022-10968-y.

[25] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Towards an effective baseline of it governance mechanisms in higher education institution," in *17th International Conference on e-Learning and Digital Learning*, Porto, Portugal, Jul. 2023, pp. 107–116, https://doi.org/10.33965/EL_STE2023_202303L014.

[26] B. R. Aditya, R. Ferdiana, and S. S. Kusumawardani, "The Study of the Barriers to Digital Transformation in Higher Education: A Preliminary Investigation in Indonesia," in *6th International Conference on Science and Technology*, Yogyakarta, Indonesia, Sep. 2020, vol. 1, pp. 1–6, https://doi.org/10.1109/ICST50505.2020.9732809.

[27] M. S. Khan, M. Hasan, and C. Clement, "Barriers to the Introduction of ICT into Education in Developing Countries: The Example of Bangladesh," *International Journal of Instruction*, vol. 5, no. 2, pp. 61–80, Jul. 2012.

[28] K. Watty, J. McKay, and L. Ngo, "Innovators or inhibitors? Accounting faculty resistance to new educational technologies in higher education," *Journal of Accounting Education*, vol. 36, pp. 1–15, Sep. 2016, https://doi.org/10.1016/j.jaccedu.2016.03.003.

[29] J. Sinclair and A.-M. Aho, "Experts on Super Innovators: Understanding Staff Adoption of Learning Management Systems," *Higher Education Research and Development*, vol. 37, no. 1, pp. 158–172, 2018, https://doi.org/10.1080/07294360.2017.1342609.

[30] S. Ahriz, N. Benmoussa, A. E. Yamami, K. Mansouri, and M. Qbadou, "An Elaboration of a Strategic Alignment Model of University Information Systems based on SAM Model," *Engineering, Technology & Applied Science Research*, vol. 8, no. 1, pp. 2471–2476, Feb. 2018, https://doi.org/10.48084/etasr.1696.

[31] P. Reid, "Categories for barriers to adoption of instructional technologies," *Education and Information Technologies*, vol. 19, no. 2, pp. 383–407, Jun. 2014, https://doi.org/10.1007/s10639-012-9222-z.

[32] B. R. Aditya, R. Ferdiana, and S. S. Kusumawardani, "Barriers to Digital Transformation in Higher Education: An Interpretive Structural Modeling Approach," *International Journal of Innovation and Technology Management*, vol. 18, no. 5, Aug. 2021, Art. no. 2150024, https://doi.org/10.1142/S0219877021500243.

[33] S. Packmohr and H. Brink, "Impact of the Pandemic on the Barriers to the Digital Transformation in Higher Education - Comparing Pre- and Intra-Covid-19 Perceptions of Management Students," in *International Conference on Business Informatics Research*, Vienna, Austria, Sep. 2021, pp. 3–18, https://doi.org/10.1007/978-3-030-87205-2_1.

[34] M. A. Sanchez, "University E-readiness for the Digital Transformation: the Case of Universidad Nacional del Sur," *Revista Gestao & Tecnologia*, vol. 20, no. 2, pp. 75–97, May 2020, https://doi.org/10.20397/2177-6652/2020.v20i2.1848.

[35] M. Alenezi, "Deep Dive into Digital Transformation in Higher Education Institutions," *Education Sciences*, vol. 11, no. 12, Dec. 2021, Art. no. 770, https://doi.org/10.3390/educsci11120770.

[36] C. Abdelilah, A. Souad, K. El Guemmat, and K. Mansouri, "Evaluating IT Governance in the DSS Domain (Delivery, Service, and Support) through COBIT 5 Framework at a Moroccan University," in *4th International Conference on Innovative Research in Applied Science, Engineering and Technology*, FEZ, Morocco, Dec. 2024, pp. 1–5, https://doi.org/10.1109/IRASET60544.2024.10548341.

[37] B. R. Aditya, R. Ferdiana, and S. S. Kusumawardani, "Categories for Barriers to Digital Transformation in Higher Education: An Analysis Based on Literature," *International Journal of Information and Education Technology*, vol. 11, no. 12, pp. 658–664, 2021, https://doi.org/10.18178/ijiet.2021.11.12.1578.

[38] A. Marks, M. AL-Ali, R. Atassi, A. A. Elkishk, and Y. Rezgui, "Digital Transformation in Higher Education: Maturity and Challenges Post COVID-19," in *International Conference on Information Technology & Systems*, Libertad, Ecuador, Feb. 2021, pp. 53–70, https://doi.org/10.1007/978-3-030-68285-9_6.

[39] M. Rafiq, S. H. Batool, A. F. Ali, and M. Ullah, "University libraries response to COVID-19 pandemic: A developing country perspective," *The Journal of Academic Librarianship*, vol. 47, no. 1, Jan. 2021, Art. no. 102280, https://doi.org/10.1016/j.acalib.2020.102280.

[40] M. Kopp, O. Groblinger, and S. Adams, "Five common assumptions that prevent digital transformation at higher education institutions," in *INTED2019 Conference*, Valencia, Spain, Mar. 2019, pp. 1448–1457, https://doi.org/10.21125/inted.2019.0445.

[41] A. Chahid, S. Ahriz, K. el Guemmat, and K. Mansouri, "Implementation of suitable information technology governance frameworks for Moroccan higher education institutions," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3116–3126, Jun. 2024, https://doi.org/10.11591/ijece.v14i3.pp3116-3126.

[42] T. Gkrimpizi and V. Peristeras, "Barriers to digital transformation in higher education institutions," in *15th International Conference on Theory and Practice of Electronic Governance*, Guimaraes, Portugal, Oct. 2022, pp. 154–160, https://doi.org/10.1145/3560107.3560135.

[43] A. Lasakova, Ľ. Bajzikova, and I. Dedze, "Barriers and drivers of innovation in higher education: Case study-based evidence across ten European universities," *International Journal of Educational Development*, vol. 55, pp. 69–79, Jul. 2017, https://doi.org/10.1016/j.ijedudev.2017.06.002.

[44] B. Alzahrani, H. Bahaitham, M. Andejany, and A. Elshennawy, "How Ready Is Higher Education for Quality 4.0 Transformation according to the LNS Research Framework?," *Sustainability*, vol. 13, no. 9, Jan. 2021, Art. no. 5169, https://doi.org/10.3390/su13095169.

[45] J. Stuber, "Barriers of Digital Technologies in Higher Education : A Teachers' Perspective from a Swedish University," M.S. thesis, Linnaeus University, Smaland, Sweden, 2018.

[46] A. Chahid, S. Ahriz, K. El Guemmat, and K. Mansouri, "Building a Specialized IT Governance Strategy for Higher Education: A Strategic Model," *Journal of Computer Science*, vol. 20, no. 7, pp. 768–782, May 2024, https://doi.org/10.3844/jcssp.2024.768.782.

[47] J. Chapman, "How safe is your data? Cyber-security in higher education," HEPI, HEPI Policy Note 12, Apr. 2019.

[48] G. Wangen, "Quantifying and Analyzing Information Security Risk from Incident Data," in *International Workshop on Graphical Models for Security*, Hoboken, NJ, USA, Jun. 2019, pp. 129–154, https://doi.org/10.1007/978-3-030-36537-0_7.

[49] H. Durojaye and O. Raji, "Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure." arXiv, Dec. 13, 2022, https://doi.org/10.48550/arXiv.2212.08036.

[50] G. Wangen, E. Ø. Brodin, B. H. Skari, and C. Berglind, "Unrecorded security incidents at NTNU 2018 (Mørketallsundersøkelsen ved NTNU 2018)," vol. 17, 2019.

[51] J. Grama, "Just in Time Research: Data Breaches in Higher Education," EDUCAUSE, 2014.

[52] A. D. Shearry-Sneed, "A Case Study on the Benefits and Barriers of Information Security Knowledge Sharing in Higher Education

Institutions," Ph.D. dissertation, Northcentral University, San Diego, CA, USA, 2018.

[53] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities," *Applied Sciences*, vol. 9, no. 21, Jan. 2019, Art. no. 4479, https://doi.org/10.3390/app9214479.

[54] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, G. Giannakopoulos, and C. Skourlas, "Human factor and information security in higher education," *Journal of Systems and Information Technology*, vol. 16, no. 3, pp. 210–221, Aug. 2014, https://doi.org/10.1108/JSIT-01-2014-0007.

[55] T. L. Saaty, "Fundamentals of the analytic network process — Dependence and feedback in decision-making with a single network," *Journal of Systems Science and Systems Engineering*, vol. 13, no. 2, pp. 129–157, Apr. 2004, https://doi.org/10.1007/s11518-006-0158-y.

[56] N. Tiwari, "Using the analytic hierarchy process (AHP) to identify performance scenarios for enterprise application," *Measure It*, vol. 4, no. 3, 2006.

[57] L. Saaty, "The analytic hierarchy process (AHP)," *The Journal of the Operational Research Society*, vol. 41, pp. 1073–1076, 1980.

[58] T. L. Saaty, *Theory and Applications of the Analytic Network Process: Decision Making With Benefits, Opportunities, Costs, and Risks*. Pittsburgh, PA, USA: RWS Publications, 2005.

[59] T. L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process," *Interfaces*, vol. 24, no. 6, pp. 19–43, Dec. 1994, https://doi.org/10.1287/inte.24.6.19.

[60] A. Dias and P. G. Ioannou, "Company and Project Evaluation Model for Privately Promoted Infrastructure Projects," *Journal of Construction Engineering and Management*, vol. 122, no. 1, pp. 71–82, Mar. 1996, https://doi.org/10.1061/(ASCE)0733-9364(1996)122:1(71).

[61] J. M. Duke and R. Aull-Hyde, "Identifying public preferences for land preservation using the analytic hierarchy process," *Ecological Economics*, vol. 42, no. 1, pp. 131–145, Aug. 2002, https://doi.org/10.1016/S0921-8009(02)00053-8.

[62] R. K. Shrestha, J. R. R. Alavalapati, and R. S. Kalmbacher, "Exploring the potential for silvopasture adoption in south-central Florida: an application of SWOT–AHP method," *Agricultural Systems*, vol. 81, no. 3, pp. 185–199, Sep. 2004, https://doi.org/10.1016/j.agsy.2003.09.004.

[63] W. Purwanto, H. Wu, M. Sosonkina, and K. Arcaute, "DeapSECURE: Empowering Students for Data- and Compute-Intensive Research in Cybersecurity through Training," in *PEARC '19: Practice and Experience in Advanced Research Computing*, Chicago, IL, USA, Aug. 2019, pp. 1–8, https://doi.org/10.1145/3332186.3332247.

[64] S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions," in *Proceedings of the Cyber Secure Nigeria Conference*, Abuja, Nigeria, Jul. 2023, pp. 151–160.

[65] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence," *Information Systems Frontiers*, vol. 23, no. 2, pp. 361–373, Apr. 2021, https://doi.org/10.1007/s10796-019-09977-z.

[66] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based Cybersecurity Training for High School Students," in *49th ACM Technical Symposium on Computer Science Education*, Baltimore, MD, USA, Feb. 2018, pp. 68–73, https://doi.org/10.1145/3159450.3159591.

[67] T. Gkrimpizi, V. Peristeras, and I. Magnisalis, "Classification of Barriers to Digital Transformation in Higher Education Institutions: Systematic Literature Review," *Education Sciences*, vol. 13, no. 7, Jul. 2023, Art. no. 746, https://doi.org/10.3390/educsci13070746.

[68] M. Matsieli and S. Mutula, "COVID-19 and Digital Transformation in Higher Education Institutions: Towards Inclusive and Equitable Access to Quality Education," *Education Sciences*, vol. 14, no. 8, Aug. 2024, Art. no. 819, https://doi.org/10.3390/educsci14080819.

[69] N. C. Jackson, "Managing for competency with innovation change in higher education: Examining the pitfalls and pivots of digital transformation," *Business Horizons*, vol. 62, no. 6, pp. 761–772, Nov. 2019, https://doi.org/10.1016/j.bushor.2019.08.002.

[70] F. R. Akbar, Sasmoko, E. A. Kuncoro, and V. U. Tjhin, "Digital Transformation Readiness In Indonesian Institutions Of Higher Education With Digital Enabler," *Migration Letters*, vol. 21, no. S3, pp. 297–306, Jan. 2024.

[71] B. Rima Aditya, R. Ferdiana, and S. Suning Kusumawardani, "Digital Transformation in Higher Education: A Barrier Framework," in *3rd International Conference on Modern Educational Technology*, Jakarta, Indonesia, Dec. 2021, pp. 100–106, https://doi.org/10.1145/3468978.3468995.

[72] F. Ozsungur, "Business Management and Strategy in Cybersecurity for Digital Transformation," in *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, Hershey, PA, USA: IGI Global, 2021, pp. 144–162.

[73] K. A. Y. Yaseen, "Importance of Cybersecurity in The Higher Education Sector 2022," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20–24, Oct. 2022, https://doi.org/10.51983/ajcst-2022.11.2.3448.

[74] D. Polemi and K. Kioskli, "Enhancing practical cybersecurity skills: The ECSF and the CyberSecPro European efforts," *Human Factors in Cybersecurity*, vol. 91, pp. 93–100, Jan. 2023, https://doi.org/10.54941/ahfe1003723.