REPOSITIONING THE ROLE OF PRIVATE UNIVERSITIES IN COMBATING SOCIAL EVILS IN CYBERSPACE: *DRIVING FORCE FROM OPEN SCIENCE, ARTIFICIAL INTELLIGENCE AND GLOBAL DIGITAL TRANSFORMATION*

Ngo Quang Son*
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: ngoquangson2018@gmail.com
ORCID iD: https://orcid.org/0000-0003-3120-034X

Pham Thi Thanh*
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: thanhpt153@gmail.com
ORCID iD: https://orcid.org/0009-0008-6452-4766

Pham Thi Van Anh
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: vananhltv86@gmail.com
ORCID iD: https://orcid.org/0009-0009-0982-2434

Bui Thi Huong
Institute of Applied Psychology, Ho Chi Minh City
Email: vientamlyungdung@gmail.com
ORCID iD: https://orcid.org/0009-0001-7164-0051

Pham Thu Ha
Nguyen Trai University
Email: hathu30789@gmail.com
ORCID iD: https://orcid.org/0009-0001-1563-8766

Le Thi Ly Na
Lam Dong Department of Education and Training
Email: lynavn89@gmail.com
ORCID iD: https://orcid.org/0009-0009-2715-2307

Trinh Minh Truong
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: tmtruong@moet.gov.vn
ORCID iD: https://orcid.org/0009-0001-1622-5859

Nguyen Cong Quan
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: ncquan@gmail.com
ORCID iD: https://orcid.org/0009-0001-0890-2178

Abstract:

In the context of global digital transformation, open science, and the rapid advancement of artificial intelligence (AI), cyberspace has emerged as both a catalyst for knowledge innovation and a breeding ground for digital social threats, including misinformation, cyberbullying, online fraud, data privacy violations, and other forms of online social deviance. These challenges have imposed increasing responsibilities on higher education institutions, particularly private universities, to reposition their roles in fostering safe, ethical, and sustainable digital academic ecosystems.

This study examines the strategic role of private universities in combating cyber-social deviance through interdisciplinary approaches encompassing digital university governance, open science, digital citizenship education, and knowledge security. The research employs a qualitative methodology integrating policy analysis, international literature review, and comparative approaches to explore governance models, educational mechanisms, and adaptive capacities of private higher education institutions in the era of global digital transformation.

The findings indicate that private universities possess significant potential to act as pioneering institutions in promoting digital ethics, strengthening cyber-risk awareness, advancing safe academic cultures, and cultivating responsible digital learning environments. Furthermore, the study proposes an integrated governance framework that combines AI, open science, and digital citizenship education to enhance the effectiveness of cyber-social threat prevention in higher education.

The study contributes theoretically and practically by extending scholarly discourse on digital universities, digital social security, and the social responsibility of higher education institutions within the global knowledge society.

Keywords: *Private universities; Social evils in cyberspace; Open science; Artificial intelligence; Global digital transformation.*

UNESCO FOS: 5802, 5311, 120304, 120310.
JEL Codes: I23, O33, D83, L86;
UNESCO Codes: 5312.90, 5312.04, 1203.24, 3325.05

Tran Thi Hue
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: lily071081@gmail.com
ORCID iD: https://orcid.org/0009-0009-1891-1498

Nguyen Thi Hiep
Trung Vuong University
ROR ID: https://ror.org/05xzsm645
Email: Hrhiepngoc@gmail.com
ORCID iD: https://orcid.org/0009-0009-1161-8205

Article History
Received: 10/3/2026
Reviewed: 28/4/2026
Revised: 10/6/2026
Acceped: 20/6/2026
Released: 30/6/2026

DOI: https://doi.org/10.64223/tvj.p2026.v2.i6.a104

1. Introduction

1.1. Global Context

In the early decades of the twenty-first century, the simultaneous advancement of the Fourth Industrial Revolution, the emergence of an AI-driven society, the expansion of the Open Knowledge Economy, the rise of hyper-connectivity, and the pervasive process of datafication have collectively created an unprecedented digital ecosystem. Breakthroughs in artificial intelligence, cloud computing, big data analytics, the Internet of Things, and cross-border digital infrastructures are fundamentally reshaping production systems, governance mechanisms, social interactions, higher education, scientific research, and innovation ecosystems worldwide.

Nevertheless, alongside these transformative opportunities, cyberspace has increasingly evolved into a breeding ground for sophisticated forms of social deviance and cyber-enabled crime. Emerging threats - including cyber fraud, deepfake technologies, AI-generated misinformation, cyberbullying, the expanding dark web economy, and the large-scale exploitation of personal data - pose significant challenges to national security, public trust, and the sustainable development of the global digital society. The convergence of generative artificial intelligence and digital communication platforms has further accelerated the dissemination of disinformation, intensified cognitive manipulation, and expanded the operational capabilities of transnational cybercriminal networks.

Against this backdrop, the international academic community has reached a growing consensus that artificial intelligence should no longer be viewed merely as a technological instrument but rather as a transformative force fundamentally restructuring global higher education. Universities are rapidly evolving from conventional educational institutions into data-driven and innovation-oriented digital ecosystems grounded in the principles of Open Science and digital transformation. Simultaneously, they occupy a dual and increasingly critical position: as vulnerable targets of cyber threats and as strategic actors responsible for advancing research, cultivating digital competencies, developing technological solutions, and disseminating knowledge to prevent, detect, and combat cyber-enabled social problems. Consequently, there is an urgent need to reconceptualize the role of higher education institutions - particularly private universities - as pivotal stakeholders in fostering a secure, resilient, and sustainable digital society in the era of artificial intelligence and global digital transformation.

1.2. Research Gap

Despite the growing scholarly interest in cybersecurity and cyber-enabled crime over the past decade, the existing body of international literature has predominantly concentrated on technological and regulatory dimensions, including cybersecurity technology, cyber law, artificial intelligence systems, and digital governance. These studies have substantially advanced the development of security architectures, legal frameworks, and digital governance mechanisms; however, they remain largely technology-centric or policy-oriented and have paid comparatively limited attention to the strategic role of higher education institutions in preventing and mitigating cyber-enabled social problems.

A particularly significant research gap lies in the insufficient examination of the role of private universities within the broader ecosystem of digital security and cyber risk governance. As private higher education institutions continue to expand their academic capacity, strengthen innovation ecosystems, and intensify collaborations with industry and international partners, the lack

of systematic investigation into their potential contributions has constrained both theoretical understanding and policy development regarding their role in addressing cyber-related social challenges.

Furthermore, current scholarship has yet to establish an integrated framework that combines Open Science, Artificial Intelligence, and Cyber Prevention into a coherent and synergistic model capable of linking scientific research, knowledge sharing, technological innovation, and digital community protection. This omission is particularly consequential in an era where AI-driven technologies and open data infrastructures are increasingly recognized as fundamental drivers of global higher education transformation and intelligent societal governance.

Equally important, the literature has not proposed a comprehensive university governance framework specifically designed to combat cyber-enabled social problems, encompassing strategic leadership, digital talent development, responsible digital culture, multi-stakeholder collaboration, and data-driven institutional management. The absence of such a holistic governance paradigm highlights the urgent need for new conceptual and practical models that reposition private universities as innovation hubs, knowledge producers, and proactive actors in safeguarding digital society.

Against this backdrop, the present study seeks to bridge these critical research gaps by advancing an interdisciplinary and multidimensional perspective on the strategic role of private universities in preventing cyber-enabled social problems. It further proposes an integrated framework that synthesizes Open Science, Artificial Intelligence, and Global Digital Transformation as a novel theoretical and practical foundation for university governance in the digital age.

1.3. Research Questions

Building upon the global context of digital transformation, the rapid advancement of artificial intelligence and Open Science, and the research gaps identified in previous studies, this article aims to clarify the strategic role of private universities in preventing cyber-enabled social problems through the following core research questions.

RQ1. How can private universities be repositioned within the ecosystem of cyber-enabled social problem prevention?

This question explores the potential transformation of private higher education institutions from conventional educational providers into proactive actors that foster digital awareness, generate technological innovation, disseminate knowledge, and facilitate multi-stakeholder collaboration to prevent, detect, and mitigate cyber-enabled social problems.

RQ2. How do Artificial Intelligence, Open Science, and Digital Transformation influence the cyber prevention capabilities of universities?

This question investigates the mechanisms through which advanced digital technologies, open knowledge ecosystems, and digital transformation strategies enhance universities' capacities for research, education, risk prediction, early detection, and effective intervention in addressing cyber-enabled social threats.

RQ3. Which factors determine the effectiveness of the "Cyber Prevention University" model?

The objective of this question is to identify and evaluate the critical determinants shaping the success of a university-oriented cyber prevention model, including strategic leadership and governance, digital infrastructure, high-quality human capital, responsible digital culture, interdisciplinary collaboration, international partnerships, and the integration of artificial intelligence and Open Science into education, research, and community engagement.

RQ4. What governance model is most appropriate for developing the "Cyber Prevention University" framework in both the Vietnamese and global contexts?

This question seeks to develop and propose an integrated university governance framework that is adaptable to Vietnam's institutional realities while simultaneously aligning with international standards of digital governance, innovation, Open Science, and sustainable development. Such a framework is expected to strengthen the role of private universities as strategic contributors to cyber-enabled social problem prevention and digital societal resilience. Collectively, these four research questions provide the conceptual foundation for the analytical framework of the study and guide the development of theoretical contributions, governance models, and policy recommendations aimed at enhancing the strategic role of private higher education institutions in the era of artificial intelligence and global digital transformation.

1.4. Research Objectives

Responding to the urgent need to redefine the role of higher education in an era shaped by artificial intelligence, Open Science, and global digital transformation, this study is designed with the overarching objective of developing a comprehensive theoretical and practical framework

to reposition private universities as strategic actors in preventing cyber-enabled social problems. In doing so, the research seeks to extend the traditional mission of higher education beyond teaching and research toward fostering digital security, strengthening societal resilience, and supporting sustainable development within the emerging digital ecosystem. To achieve this overarching objective, the study pursues a set of interconnected and complementary specific research objectives.

First, the study aims to develop a novel theoretical framework that conceptualizes the strategic role of private universities within the ecosystem of cyber-enabled social problem prevention by integrating contemporary perspectives on university governance, Open Science, artificial intelligence, and digital transformation. This framework is expected to address existing theoretical deficiencies and provide a robust foundation for future research at the intersection of higher education governance and digital security.

Second, the research proposes the "AI-enabled Cyber Prevention University" model, in which artificial intelligence serves as a core enabling technology for risk forecasting, data analytics, anomaly detection, personalized digital literacy education, and evidence-based institutional governance. The proposed model also incorporates the principles of Open Science to promote knowledge sharing, collaborative research, and innovation-oriented solutions for the broader public good.

Third, the study seeks to evaluate the level of digital readiness among private universities with respect to their capacity to prevent cyber-enabled social problems by examining critical dimensions such as digital infrastructure, governance capability, human resources, data ecosystems, and stakeholder collaboration within the digital environment.

Fourth, the research focuses on analyzing institutional capabilities in Artificial Intelligence and Open Science across education, scientific research, university governance, and community engagement in order to assess how these capabilities contribute to strengthening universities' effectiveness in preventing and responding to cyber-enabled social challenges.

Finally, drawing upon both theoretical insights and empirical evidence, the study aims to propose a national policy framework that supports the strategic repositioning of private universities within broader cyber prevention and digital security strategies. This policy framework is envisioned as an integrated approach combining higher education reform, digital transformation, high-quality human resource development, data-driven governance, and cross-sector collaboration to advance a secure, inclusive, and sustainable digital society.

2. Literature Review

2.1. Theoretical Foundations

This study adopts an interdisciplinary theoretical perspective by integrating Open Science, Digital Transformation, Artificial Intelligence, Situational Crime Prevention, Entrepreneurial University, Civic University, and Socio-technical Systems theories to explain the evolving role of private higher education institutions in addressing the growing complexity of cyber-enabled social deviance and online social harms.

First, Open Science Theory emphasizes transparency, accessibility, collaboration, and the open sharing of scientific knowledge, research data, and innovation resources. Within the context of cybercrime and online social harm prevention, open science facilitates the development of collaborative knowledge ecosystems in which universities, policymakers, technology companies, and civil society organizations jointly generate evidence-based solutions to emerging digital threats.

Second, Digital Transformation Theory argues that digitalization extends far beyond technological adoption, encompassing profound organizational, cultural, managerial, and strategic changes. From this perspective, private universities are increasingly transforming from traditional educational institutions into digitally enabled innovation hubs capable of mobilizing technological resources to address complex societal challenges, including cybercrime, online fraud, digital misinformation, and other forms of cyber-enabled social misconduct.

Complementing this perspective, Artificial Intelligence Theory provides the conceptual foundation for leveraging machine learning, predictive analytics, and big data technologies to detect abnormal patterns, identify emerging risks, and support proactive intervention strategies. AI functions not merely as a technological tool but as an intelligent decision-support system that enhances institutional capacity for cyber risk management, digital governance, and social protection.

A particularly relevant framework is Situational Crime Prevention (SCP) Theory, which posits that criminal behavior is significantly influenced by environmental opportunities. Crime can be reduced by increasing effort, increasing risk, reducing rewards, and eliminating situational conditions that facilitate offending. In cyberspace, SCP offers valuable insights into designing safer digital environments through awareness-building initiatives, technological safeguards, behavioral

regulation mechanisms, and enhanced cybersecurity infrastructures.

Furthermore, Entrepreneurial University Theory suggests that contemporary universities should transcend their traditional missions of teaching and research to become active agents of innovation and societal transformation. Under this framework, private universities can contribute to cybercrime prevention through the creation of AI-driven solutions, digital innovation platforms, and cross-sector partnerships that generate measurable social impact.

Simultaneously, Civic University Theory highlights the public responsibility of higher education institutions in addressing societal challenges. Universities are expected not only to produce knowledge but also to foster civic engagement, digital citizenship, ethical awareness, and social resilience. Consequently, private universities possess significant potential to become influential actors in promoting safe, inclusive, and responsible digital communities.

Finally, Socio-technical Systems Theory provides a holistic analytical framework that integrates technological, human, organizational, and institutional dimensions. The theory argues that technological effectiveness depends on the alignment between digital systems, human behavior, governance structures, and organizational culture. Accordingly, effective cybercrime prevention requires a coordinated ecosystem involving universities, government agencies, industry stakeholders, and civil society organizations.

Drawing upon these complementary theoretical perspectives, this study proposes a novel conceptualization of private universities as Digital Social Innovation Hubs, capable of leveraging Open Science, Artificial Intelligence, and Digital Transformation to proactively prevent, detect, and mitigate cyber-enabled social problems in an increasingly interconnected global digital society.

2.2. Private Universities in the Digital Era

Amid the unprecedented acceleration of the Fourth Industrial Revolution and global digital transformation, private universities are increasingly compelled to redefine their missions, governance structures, and societal responsibilities. While universities have traditionally been viewed as institutions for knowledge creation and human capital development, contemporary higher education institutions—particularly private universities - are evolving into innovation-driven organizations capable of generating technological solutions and addressing complex societal challenges (Altbach, Reisberg, & de Wit, 2019).

A fundamental driver of this transformation is university autonomy. According to de Boer, Enders, and Schimank (2007), university autonomy encompasses not only academic, financial, and administrative independence but also the strategic capacity to respond effectively to rapidly changing external environments. For private universities, greater autonomy enables institutional agility, accelerates digital transformation initiatives, and supports the development of innovative governance models capable of responding to emerging societal risks in the digital age.

Alongside institutional autonomy, AI governance has emerged as a critical component of modern university management. UNESCO (2021) defines AI governance as the framework of principles, policies, and accountability mechanisms designed to ensure that artificial intelligence is developed and deployed in ways that are ethical, transparent, inclusive, and human-centered. Within higher education, AI governance extends beyond the adoption of intelligent technologies and encompasses issues of digital ethics, data protection, algorithmic accountability, and responsible innovation. Consequently, private universities are increasingly expected to become leaders in establishing ethical and socially responsible AI ecosystems.

Another prominent development is the emergence of the Smart Campus paradigm. Smart campuses integrate Internet of Things (IoT) technologies, artificial intelligence, cloud computing, and data analytics to optimize learning, research, and administrative processes (Kwok, 2015). Beyond operational efficiency, smart campuses create digitally secure environments capable of monitoring risks, identifying abnormal behaviors, and enhancing institutional resilience against cyber threats. Such capabilities are particularly relevant in addressing the growing prevalence of cyber-enabled social problems.

Concurrently, the concept of the Digital University has gained significant attention in international scholarship. According to Bond et al. (2018), digital universities represent a comprehensive transformation that extends beyond technological adoption to encompass organizational culture, governance systems, pedagogical innovation, and knowledge ecosystems. Through data-driven decision-making and digitally enabled collaboration, universities become active contributors to broader societal innovation and sustainable development.

Moreover, contemporary higher education research increasingly emphasizes the importance of Open Innovation Ecosystems. Chesbrough (2003) argues that innovation is most effective when organizations leverage both internal and

external knowledge resources through collaborative networks. In higher education contexts, open innovation ecosystems facilitate partnerships among universities, industry, government agencies, civil society organizations, and local communities. Recent studies by Secundo et al. (2021) demonstrate that universities are becoming central nodes within open innovation networks, generating collective intelligence and co-creating solutions to complex societal challenges.

The international literature therefore suggests a profound transition from viewing private universities as educational service providers to recognizing them as digital social innovation actors. The convergence of university autonomy, AI governance, smart campus development, digital university transformation, and open innovation ecosystems provides a robust foundation for private universities to play a proactive role in preventing, detecting, and mitigating cyber-enabled social harms in the era of global digital transformation.

2.3. Artificial Intelligence and the Prevention of Cyber-Enabled Social Harms

The rapid advancement of Artificial Intelligence (AI) is fundamentally transforming how organizations and societies detect, prevent, and respond to threats in cyberspace. As cyber-enabled social harms - including online fraud, misinformation, cyberbullying, child exploitation, digital radicalization, and cybercrime - become increasingly sophisticated, AI has emerged as a strategic technology capable of enhancing prediction, early detection, and intervention capabilities (Russell & Norvig, 2021).

One of the most significant applications of AI lies in threat detection. Machine learning and deep learning algorithms can process massive volumes of real-time data and identify anomalies that may remain undetected through conventional approaches. Sommer and Paxson (2010) demonstrated that machine learning techniques substantially improve cyber threat detection by learning behavioral patterns associated with malicious activities. More recent studies indicate that AI-powered intrusion detection systems have become essential components of next-generation cybersecurity infrastructures, enabling faster response times and reducing false-positive rates (Buczak & Guven, 2016).

Simultaneously, the proliferation of generative AI technologies has intensified concerns regarding the creation of highly convincing synthetic content, particularly deepfakes. According to Chesney and Citron (2019), deepfakes represent a significant threat to public trust, democratic institutions, and societal stability. In response, AI has also become a powerful tool for deepfake identification, employing advanced neural networks to analyze inconsistencies in facial movements, speech patterns, visual artifacts, and digital footprints. Mirsky and Lee (2021) found that deep learning models can achieve high levels of accuracy in detecting manipulated content, thereby contributing to efforts aimed at combating digital deception and misinformation.

Another rapidly expanding field is behavioral analytics. Unlike traditional security approaches that focus primarily on devices or network infrastructures, AI-driven behavioral analytics examines patterns of human activity to identify suspicious or harmful behavior. Eberle and Holder (2009) argue that behavioral pattern mining enables the early detection of fraud, cyber harassment, online extremism, and other forms of deviant behavior. Within higher education environments, behavioral analytics can support the identification of cyberbullying risks, problematic online engagement, and emerging digital well-being concerns among students.

Furthermore, AI is driving major advances in predictive cybersecurity. Rather than reacting to incidents after they occur, predictive cybersecurity employs machine learning models to anticipate potential attacks before they materialize. Sarker (2022) highlights that the integration of big data analytics, predictive modeling, and AI technologies enables organizations to develop proactive early-warning systems capable of forecasting cyber threats, assessing vulnerabilities, and recommending preventive actions. This shift reflects a broader transition from reactive defense strategies toward proactive cyber resilience.

In addition, AI serves as the foundation for intelligent monitoring systems. AI-enabled monitoring platforms can automatically collect, process, and evaluate data from multiple digital environments to detect harmful content, suspicious activities, and emerging social risks. Kshetri (2021) notes that intelligent monitoring technologies are increasingly utilized in cybersecurity management, online child protection, fraud prevention, and digital risk governance. Nevertheless, scholars emphasize that such systems must be implemented in accordance with ethical AI principles, privacy protection standards, and human rights considerations (UNESCO, 2021).

Overall, the international literature suggests that AI is evolving from a supportive technological tool into a strategic foundation for cyber social harm prevention ecosystems. Through threat detection, deepfake identification, behavioral analytics, predictive cybersecurity, and intelligent monitoring, AI facilitates a paradigm shift from

reactive responses toward proactive prediction and prevention. This transformation creates significant opportunities for private universities to contribute through research, innovation, education, and multi-stakeholder collaboration aimed at fostering safer, more ethical, and more resilient digital societies.

2.4. Open Science and Digital Knowledge Security

The emergence of the knowledge economy and the acceleration of global digital transformation have positioned Open Science as one of the most influential scholarly movements of the twenty-first century. According to UNESCO (2021), Open Science promotes transparency, accessibility, collaboration, and the reusability of scientific knowledge, thereby democratizing access to research outputs and fostering inclusive innovation. Within digitally connected societies, Open Science contributes to the development of global knowledge ecosystems in which data, technologies, and expertise can be shared across institutional and national boundaries.

One of the fundamental pillars of Open Science is Open Data. Uhlir and Schröder (2007) argue that open access to scientific data enhances transparency, reproducibility, and research efficiency by enabling researchers and institutions to reuse and validate existing datasets. In the context of cybersecurity and cyber-enabled social harm prevention, open data facilitates the analysis of cybercrime trends, supports anomaly detection, and strengthens evidence-based approaches to digital risk management.

Another key component is the development of Open Repositories, which have become critical infrastructures for contemporary scholarly communication. Lynch (2003) emphasizes that open repositories not only preserve scientific outputs but also facilitate the dissemination of research articles, datasets, software, and educational resources. For universities operating in digital environments, open repositories enhance knowledge visibility, foster collaboration, and support innovation ecosystems capable of addressing complex societal challenges.

Closely related to these developments is the principle of Knowledge Transparency. According to Fecher and Friesike (2014), transparency in scientific processes is essential for strengthening trust, accountability, and reproducibility within the research community. By openly sharing methodologies, data, and findings, researchers enable critical scrutiny and collective knowledge improvement. In cyber social harm prevention, knowledge transparency contributes to risk awareness, public education, and evidence-informed policymaking.

More recently, scholars have highlighted the importance of Collaborative Cybersecurity Intelligence as an emerging manifestation of Open Science in digital security. The European Union Agency for Cybersecurity (ENISA, 2023) argues that the sharing of threat intelligence, vulnerability information, attack patterns, and mitigation strategies significantly enhances collective cyber resilience. Collaborative intelligence networks involving universities, technology firms, government agencies, and research communities are increasingly recognized as effective mechanisms for strengthening cybersecurity preparedness and response capabilities.

Despite its transformative potential, Open Science also raises significant challenges for Digital Knowledge Security. One of the most critical concerns involves Data Leakage. According to the OECD (2021), the uncontrolled release of research data may expose sensitive information, increase cybersecurity risks, and generate unintended consequences for individuals, institutions, and society. These risks are particularly pronounced in higher education environments where large volumes of research and personal data are routinely generated and exchanged.

A second challenge concerns Privacy Ethics. Floridi and Taddeo (2016) contend that expanding access to data must be balanced with the protection of privacy rights, informed consent, and ethical data governance. As artificial intelligence and big data analytics become increasingly integrated into research and institutional management, maintaining an appropriate balance between openness and privacy represents a critical policy and ethical challenge.

Furthermore, the growing reliance on open-source technologies has intensified concerns regarding **Open-source Vulnerabilities**. Recent evidence indicates that cyberattacks targeting software supply chains and open-source ecosystems are increasing worldwide (Sonatype, 2024). Although open-source software remains a cornerstone of innovation and scientific collaboration, inadequate security auditing, maintenance, and vulnerability management can transform open infrastructures into targets for sophisticated cyberattacks.

Overall, international scholarship suggests that Open Science and Digital Knowledge Security should not be viewed as competing objectives but rather as complementary dimensions of a sustainable digital knowledge ecosystem. Achieving this balance requires integrating openness, scientific transparency, cybersecurity, ethical governance, privacy protection, and responsible AI practices. Such an integrated approach is particularly relevant

for private universities seeking to reposition themselves as responsible digital social innovation hubs capable of contributing to cyber social harm prevention in the age of data-driven transformation.

2.5. Theoretical Gap and the Proposed Cyber Prevention University Framework

The existing literature has generated substantial insights into digital transformation, artificial intelligence, open science, university governance, cybersecurity, and social responsibility. Research on the Entrepreneurial University primarily emphasizes innovation, knowledge transfer, and economic development (Etzkowitz, 2013), whereas the Civic University literature focuses on public engagement, social responsibility, and contributions to sustainable development (Goddard et al., 2016).

Similarly, studies on the Digital University and Smart Campus have largely concentrated on technological transformation in teaching, research, and institutional management (Bond et al., 2018). Research on AI Governance has mainly addressed algorithmic accountability, data privacy, ethical concerns, and transparency (UNESCO, 2021), while cybersecurity scholarship has predominantly focused on technical mechanisms for threat detection and cyber defense. Open Science research, meanwhile, has highlighted knowledge sharing, data accessibility, and collaborative innovation (Fecher & Friesike, 2014). Despite these valuable contributions, several significant theoretical gaps remain.

First, most existing frameworks adopt fragmented disciplinary perspectives and lack an integrated model connecting artificial intelligence, open science, digital governance, and the prevention of cyber-enabled social harms. Universities are typically portrayed as technology adopters rather than active agents of digital social protection.

Second, although cybersecurity research has expanded considerably, the role of private universities in preventing cyber-enabled social problems remains underexplored. Existing studies predominantly focus on governments, technology corporations, and law enforcement agencies, while the preventive capacity of higher education institutions has received limited scholarly attention.

Third, research on digital transformation and open science frequently emphasizes innovation outcomes but pays insufficient attention to the relationship between open knowledge ecosystems and societal resilience against digital risks and online social harms.

Fourth, there is currently no comprehensive theoretical framework explaining how universities can simultaneously integrate AI capabilities, open science ecosystems, ethical digital governance, and international collaboration to generate measurable societal impact in cyber social harm prevention.

To address these gaps, this study proposes a novel conceptual framework entitled the Cyber Prevention University Framework (CPUF). The framework repositions private universities not merely as educational institutions or research centers but as proactive digital social innovation actors capable of preventing, detecting, and mitigating cyber-enabled social harms.

The CPUF consists of six interconnected strategic dimensions. The first dimension, AI Capability, refers to the institutional capacity to leverage big data analytics, machine learning, predictive intelligence, and AI-driven decision support systems for identifying emerging cyber risks and supporting proactive interventions. The second dimension, Open Science Ecosystem, encompasses open data, open repositories, collaborative research networks, and interdisciplinary knowledge-sharing mechanisms. This dimension promotes collective intelligence and innovation for public benefit.

The third dimension, Digital Ethics Governance, includes policies and institutional mechanisms that ensure transparency, accountability, privacy protection, algorithmic fairness, and respect for human rights within digital environments. It serves as the normative foundation for responsible AI and Open Science implementation.

The fourth dimension, Cyber Resilience, reflects the university's ability to anticipate, withstand, respond to, recover from, and adapt to cyber threats and cyber-enabled social risks.

The fifth dimension, Community Engagement, emphasizes the university's role as a connector among students, academics, industry partners, public authorities, and civil society organizations to foster digital citizenship, cyber awareness, and collective responsibility.

The sixth dimension, Global Digital Collaboration, highlights the importance of participation in international academic networks, open innovation ecosystems, and cross-border data-sharing initiatives. Given the transnational nature of cyber threats, global collaboration is essential for strengthening collective prevention capabilities.

From a theoretical perspective, the CPUF extends Entrepreneurial University Theory, Civic University Theory, and Socio-technical Systems Theory by integrating AI, Open Science, Digital Ethics Governance, and Cyber Resilience into a unified analytical framework. From a practical perspective, the framework provides a strategic foundation for transforming private universities into

digitally empowered social innovation hubs capable of contributing directly to the prevention of cyber-enabled social harms and the promotion of safer digital societies.

3. Conceptual Framework

3.1. Proposed Research Model

Building upon Open Science Theory, Digital Transformation Theory, Artificial Intelligence Theory, Entrepreneurial University Theory, Civic University Theory, Situational Crime Prevention Theory, and Socio-technical Systems Theory, this study proposes a novel conceptual framework to explain how private universities can enhance their capacity to prevent cyber-enabled social harms in an increasingly digitalized world.

Unlike previous studies that predominantly focus on isolated technological solutions or specific governance mechanisms, the proposed framework adopts an integrated ecosystem perspective, recognizing that technological capabilities, organizational readiness, digital culture, and social responsibility collectively influence institutional contributions to cyber social protection.

The model consists of three categories of constructs: independent variables, mediating variables, and dependent variables.

Independent Variables

The first independent variable, AI Capability, refers to the university's capacity to deploy artificial intelligence for data analytics, predictive intelligence, intelligent monitoring, risk assessment, and decision support. Existing studies suggest that AI significantly enhances the detection of cyber threats and supports proactive prevention strategies (Sarker, 2022).

The second construct, Open Science Readiness, reflects the institution's preparedness to develop open data infrastructures, open repositories, collaborative research networks, and knowledge-sharing mechanisms. A mature open science ecosystem is expected to facilitate collective intelligence and evidence-based responses to cyber-enabled social challenges (UNESCO, 2021).

The third independent variable, Digital Transformation Capacity, represents the extent to which digital technologies are embedded within institutional infrastructure, governance systems, educational services, and operational processes. Higher levels of digital maturity are generally associated with greater adaptability and resilience in dynamic digital environments (Vial, 2019).

The fourth construct, Cybersecurity Governance, encompasses policies, risk-management mechanisms, security protocols, and institutional capacities aimed at protecting digital assets and ensuring cyber resilience. Effective cybersecurity governance is widely recognized as a prerequisite for sustainable digital development (Von Solms & Van Niekerk, 2013).

The fifth independent variable, Ethical Digital Culture, captures the values, norms, and behavioral standards that promote responsible technology use, AI ethics, privacy protection, and digital accountability. This dimension provides the cultural foundation for sustainable digital transformation.

Mediating Variables

The model proposes that the effects of these institutional capabilities are transmitted through three critical mediating mechanisms.

The first mediator, Digital Citizenship Education, refers to the university's ability to equip learners with the competencies, values, and ethical awareness required for responsible participation in digital environments.

The second mediator, Cyber Awareness, reflects the level of knowledge, vigilance, and preparedness among students, faculty members, and staff regarding cyber risks and online threats.

The third mediator, Institutional Resilience, represents the organization's capacity to anticipate, adapt to, withstand, and recover from technological disruptions, cyber incidents, and emerging digital risks.

Dependent Variables

The model evaluates institutional outcomes through two dependent variables.

The first dependent variable, Cybercrime Prevention Effectiveness, measures the university's effectiveness in preventing cybercrime, online fraud, cyberattacks, and other forms of unlawful digital activities.

The second dependent variable, Cyber Social Protection Capacity, captures the institution's ability to protect students and communities from cyber-enabled social harms, including misinformation, cyberbullying, online exploitation, digital radicalization, and other forms of harmful online behavior.

Theoretically, the proposed framework argues that private universities can evolve into "Cyber Prevention Universities" when they simultaneously strengthen AI capability, Open Science readiness, Digital Transformation capacity, Cybersecurity Governance, and Ethical Digital Culture. These capabilities foster Digital Citizenship Education, Cyber Awareness, and Institutional Resilience, which in turn enhance Cybercrime Prevention

Effectiveness and Cyber Social Protection Capacity. The model therefore provides a comprehensive theoretical foundation for understanding the emerging role of private universities as proactive actors in cyber social harm prevention and digital societal protection.

3.2. Research Hypotheses Development

AI Capability Hypothesis Group

Many studies have shown that AI helps improve the ability to detect threats early, identify anomalous behavior, and support cybersecurity risk prediction (Sarker, 2022; Kshetri, 2021). Therefore, the study proposes:

H1: AI Capability positively affects Cybercrime Prevention Effectiveness.

In addition, AI supports digital citizenship education through personalized learning, intelligent alerts, and learner behavior analysis.

H2: AI Capability positively affects Digital Citizenship Education.

The Open Science Readiness Hypothesis

According to UNESCO (2021), the open science ecosystem contributes to increased knowledge sharing, collective learning, and community capacity building.

H3: Open Science Readiness positively influences Cyber Awareness.

In addition, sharing data, knowledge, and experience in risk prevention helps strengthen the organization's resilience.

H4: Open Science Readiness positively influences Institutional Resilience.

Hypothesis on Digital Transformation Capacity:

Organizations with a high level of digital maturity tend to adapt better to emerging threats in the digital environment (Vial, 2019).

H5: Digital Transformation Capacity positively affects Cyber Awareness.

H6: Digital Transformation Capacity positively affects Institutional Resilience.

The Cybersecurity Governance Hypothesis Group:

An effective cybersecurity governance system helps mitigate risks and enhance the protection of the digital community.

H7: Cybersecurity Governance positively affects Institutional Resilience.

H8: Cybersecurity Governance positively affects Cybercrime Prevention Effectiveness.

Hypothesis on Ethical Digital Culture

Studies on AI ethics and digital citizenship show that ethical digital culture is a crucial foundation for responsible digital behavior (Floridi & Taddeo, 2016).

H9: Ethical Digital Culture positively affects Digital Citizenship Education.

H10: Ethical Digital Culture positively affects Cyber Social Protection Capacity.

Hypothesis group regarding mediating variables:

Digital citizenship education is seen as a crucial mechanism for transforming technological resources into digital society prevention capabilities.

H11: Digital Citizenship Education positively affects Cybercrime Prevention Effectiveness.

H12: Digital Citizenship Education positively affects Cyber Social Protection Capacity.

Cybersecurity awareness helps individuals proactively identify and respond to threats in cyberspace.

H13: Cyber Awareness positively affects Cybercrime Prevention Effectiveness.

H14: Cyber Awareness positively affects Cyber Social Protection Capacity.

Institutional resilience reflects the ability to maintain operations and adapt to digital attacks or crises

H15: Institutional Resilience positively affects Cybercrime Prevention Effectiveness.

H16: Institutional Resilience positively affects Cyber Social Protection Capacity.

The Mediation Effects Hypothesis

This research suggests that technological and managerial resources do not directly influence outcomes but are transmitted through social and educational mechanisms.

H17: Digital Citizenship Education mediates the relationship between AI Capability and Cyber Social Protection Capacity.

H18: Cyber Awareness mediates the relationship between Open Science Readiness and Cybercrime Prevention Effectiveness.

H19: Institutional Resilience mediates the relationship between Cybersecurity Governance and Cyber Social Protection Capacity.

Moderating Effects Hypothesis

The study also assumes that certain organizational capabilities can alter the magnitude of the impact between variables.

H20: Digital Transformation Capacity positively moderates the relationship between Cybersecurity

Governance and Institutional Resilience.

H21: Ethical Digital Culture positively moderates the relationship between AI Capability and Digital Citizenship Education.

H22: Global Digital Collaboration positively moderates the relationship between Open Science Readiness and Cyber Social Protection Capacity.

Theoretical Contributions of the Hypothesis System

In total, the proposed model comprises 22 research hypotheses (11 direct relationships, 5 intermediate output relationships, 3 intermediate hypotheses, and 3 moderating hypotheses). This hypothesis system expands on previous research by simultaneously integrating technological dimensions (AI, digital transformation), knowledge (open science), governance (cybersecurity, digital ethics), and education (digital citizenship, cybersecurity awareness) into a unified theoretical framework to explain the new role of private universities in combating social evils in cyberspace. Summary of Core Structural Paths

AI Capability → Digital Citizenship Education → Cyber Social Protection Capacity

Open Science Readiness → Cyber Awareness → Cybercrime Prevention Effectiveness

Cybersecurity Governance → Institutional Resilience → Cyber Social Protection Capacity

Digital Transformation Capacity → Institutional Resilience → Cybercrime Prevention Effectiveness

Ethical Digital Culture → Digital Citizenship Education → Cyber Social Protection Capacity

4. Research Methodology

4.1. Research Philosophy

Investigating the role of private universities in preventing cyber-enabled social harms requires a research philosophy capable of integrating multiple theoretical perspectives, analytical levels, and methodological traditions. Cyber social harms represent a complex socio-technical phenomenon shaped by the interactions among technology, governance, education, organizational systems, public policy, and human behavior. Accordingly, this study is grounded in Pragmatism and adopts an Interdisciplinary Approach to ensure a comprehensive understanding of the phenomenon under investigation.

Rooted in the works of Dewey (1938) and further developed by contemporary scholars such as Morgan (2007), pragmatism emphasizes the practical usefulness of knowledge rather than strict adherence to a single ontological or epistemological paradigm. Unlike positivism, which prioritizes objective measurement and causal explanation, or interpretivism, which focuses on subjective meanings and social constructions, pragmatism advocates methodological flexibility and the selection of research methods based on their capacity to address specific research problems (Creswell & Plano Clark, 2018).

This philosophical stance is particularly appropriate for the present study because its objective extends beyond describing or explaining cybercrime and cyber-enabled social harms. Instead, the study seeks to develop a novel conceptual model—the Cyber Prevention University Framework (CPUF) - that can inform both institutional practice and policy development. According to Saunders, Lewis, and Thornhill (2023), pragmatism provides a suitable foundation for research addressing real-world challenges characterized by complexity, uncertainty, and rapid technological change.

In addition to pragmatism, the study adopts an Interdisciplinary Approach. Contemporary research increasingly recognizes that digital challenges such as cybercrime, misinformation, online radicalization, cyberbullying, and digital exploitation cannot be adequately understood through the lens of a single academic discipline (Klein, 2021). These phenomena emerge at the intersection of computer science, cybersecurity, data science, education, sociology, psychology, law, ethics, and public governance.

Klein (2021) argues that interdisciplinarity involves more than simply combining disciplines; it requires the integration of theories, methods, and knowledge systems to generate new insights into complex societal issues. In this study, interdisciplinarity is operationalized through the integration of Open Science Theory, Artificial Intelligence Theory, Digital Transformation Theory, Entrepreneurial University Theory, Civic University Theory, Situational Crime Prevention Theory, and Socio-technical Systems Theory into a unified analytical framework.

From a methodological perspective, the combination of pragmatism and interdisciplinarity enables the study to transcend the limitations of traditional disciplinary boundaries while producing knowledge that is both theoretically rigorous and practically relevant. This approach is particularly suited to the study's objective of repositioning private universities as digital social innovation actors capable of leveraging Open Science, Artificial Intelligence, and Digital Transformation to prevent cyber-enabled social harms and strengthen societal resilience in the era of global digitalization.

4.2. Research Design

To comprehensively investigate the emerging role of private universities in preventing cyber-enabled social harms, this study adopts a mixed-methods research design, specifically an exploratory sequential mixed-methods approach. This design combines the depth and contextual richness of qualitative inquiry with the explanatory and generalizable strengths of quantitative analysis, thereby enhancing the validity, robustness, and practical relevance of the findings (Creswell & Plano Clark, 2018).

The research is conducted in two interrelated phases. The first phase focuses on exploring, refining, and validating the proposed Cyber Prevention University Framework (CPUF) through qualitative methods. The second phase empirically tests the conceptual model and research hypotheses using advanced quantitative techniques.

Phase 1: Qualitative Research

The qualitative phase aims to explore key conceptual dimensions, assess contextual relevance, and refine measurement constructs.

Expert Interviews

Semi-structured interviews are conducted with experts in:

•Artificial Intelligence;

•Cybersecurity and Digital Governance;

•Digital Transformation in Higher Education;

•Open Science and Innovation;

•Higher Education Policy and Governance. Interview data are analyzed using thematic analysis to identify recurring themes, theoretical relationships, and contextual insights relevant to the development of the CPUF.

Delphi Method

Following the expert interviews, a Delphi study is employed to establish expert consensus regarding:

•The relevance of framework dimensions;

•The adequacy of proposed constructs;

•The strength of theoretical relationships;

•The applicability of the framework in higher education settings.

The Delphi technique is particularly suitable for theory building and validation in emerging interdisciplinary domains (Okoli & Pawlowski, 2004).

Policy Analysis

The study also incorporates policy analysis of international and national documents related to:

•Digital Transformation;

•Artificial Intelligence;

•Higher Education;

•Cybersecurity;

•Open Science;

•Digital Citizenship.

Policy sources include publications and strategic frameworks from organizations such as UNESCO, OECD, and European Commission. This analysis ensures that the proposed framework remains theoretically robust and policy relevant.

Phase 2: Quantitative Research

Following qualitative refinement, the quantitative phase empirically tests the conceptual model and hypotheses.

Survey

Data are collected through a structured questionnaire using five-point or seven-point Likert scales. Participants may include:

•University leaders and administrators;

•Academic staff;

•Information technology professionals;

•Digital governance officers;

•Students;

•Cybersecurity and digital transformation experts.

Structural Equation Modeling (SEM)

SEM is employed to test the overall fit of the conceptual model and examine causal relationships among latent constructs. This approach enables the simultaneous assessment of direct, indirect, and total effects within the proposed framework.

Partial Least Squares Structural Equation Modeling (PLS-SEM)

Given the exploratory nature of the CPUF and its interdisciplinary complexity, PLS-SEM is selected as the primary analytical technique. PLS-SEM is particularly appropriate for prediction-oriented research, complex models, and theory development contexts (Hair et al., 2022).

Multi-Group Analysis (MGA)

To assess model stability and contextual variations, Multi-Group Analysis is conducted across different respondent categories, including gender, institutional type, stakeholder groups, levels of digital maturity, and potentially cross-national samples. MGA enables the identification of structural differences and enhances the external validity of the proposed framework.

4.3. Sampling and Data Collection

To ensure representativeness, statistical robustness, and generalizability, this study adopts a multi-stakeholder sampling strategy consistent with the interdisciplinary nature of the Cyber Prevention University Framework (CPUF). Such an approach is particularly appropriate for research on digital ecosystems, cybersecurity governance, and higher education transformation, where multiple actors jointly contribute to cyber social protection.

Research Participants

The study targets six stakeholder groups that play critical roles in digital transformation, cybersecurity governance, and digital citizenship development within higher education institutions.

(1)Academic Staff

Academic staff are key actors in teaching, research, and digital citizenship education. Their perspectives are essential for evaluating the integration of AI, Open Science, and digital transformation within university environments.

(2)AI Experts

AI specialists provide expertise regarding artificial intelligence capability, machine learning applications, algorithmic governance, predictive analytics, and intelligent risk management.

(3)Cybersecurity Experts

Cybersecurity professionals contribute insights into cyber governance, cyber resilience, threat management, and institutional preparedness against cyber risks.

(4)University Administrators

This group includes university leaders, department heads, digital transformation officers, and institutional managers responsible for strategic planning and governance implementation.

(5)Students

Students represent the primary beneficiaries of digital citizenship education and cybersecurity awareness programs. They are also among the most active participants in digital environments and are therefore particularly exposed to cyber-enabled social risks.

(6)Technology Enterprises

Technology firms are important partners in innovation ecosystems, technology transfer initiatives, AI deployment, and cybersecurity capacity-building programs within higher education.

Sample Size

The quantitative phase is expected to obtain between 500 and 1,000 valid responses. A sample of this magnitude is considered appropriate for advanced SEM and PLS-SEM analyses because it:

•Enhances statistical power;

•Improves parameter estimation stability;

•Reduces sampling error;

•Supports complex mediation and moderation testing;

•Enables robust multi-group analysis.

The anticipated sample distribution is as follows:

Respondent Group	Expected Sample
Academic Staff	150 – 250
Students	200 – 400
University Administrators	50 – 100
AI Experts	30 – 80
Cybersecurity Experts	30 – 80
Technology Enterprises	40 – 90
Total:	**500 – 1000**

Sampling Technique

The study employs a combination of stratified sampling and purposive sampling. Participants are first categorized into stakeholder strata and subsequently selected based on expertise, professional experience, and involvement in AI, cybersecurity, digital transformation, or higher education governance. For the Delphi study, experts are selected according to the following criteria:

•Doctoral degree or equivalent professional expertise;

•Minimum five years of relevant experience;

•Academic publications or recognized professional contributions;

•Willingness to participate in multiple Delphi rounds.

The Delphi panel is expected to consist of 15–30 experts, consistent with methodological recommendations in Delphi research.

Data Collection Procedure

Data collection involves both online and offline survey administration. The questionnaire development process includes:

1.Literature-based item generation;

2.Expert review and refinement;

3.Pilot testing;

4.Instrument revision;

5.Full-scale survey deployment.

Procedural remedies are implemented to minimize common method bias, including respondent anonymity, randomized item ordering, and post hoc statistical assessments.

Research Ethics

The study adheres to internationally recognized research ethics principles, including:

•Voluntary participation;

•Informed consent;

•Right to withdraw;

•Confidentiality and privacy protection;

•Responsible use of research data.

All collected data are anonymized, securely stored, and used exclusively for academic research purposes.

4.4. Data Analysis Methods

To ensure scientific rigor, reliability, and generalizability of the Cyber Prevention University Framework (CPUF), this study employs an integrated analytical approach combining quantitative and qualitative methods, consistent with its mixed-methods research design.

1. Quantitative Analysis

(1) Reliability Analysis – Cronbach's Alpha

Cronbach's Alpha is used to assess internal consistency reliability of measurement scales. Items with low item-total correlations are removed to ensure scale validity. A threshold of $\alpha \geq 0.70$ is adopted (Hair et al., 2022).

(2) Confirmatory Factor Analysis (CFA)

CFA is applied to validate the measurement model by assessing:

•Convergent validity

•Discriminant validity

•Model fit indices (CFI, TLI, RMSEA, AVE)

This ensures construct validity and measurement robustness (Fornell & Larcker, 1981).

(3) Structural Equation Modeling (SEM)

SEM is used to simultaneously test causal relationships among latent variables, including:

•Direct effects

•Indirect effects

•Total effects

SEM is widely recognized for analyzing complex theoretical models in social sciences (Kline, 2016).

(4) Partial Least Squares SEM (PLS-SEM)

PLS-SEM is employed for:

•Prediction-oriented modeling

•Complex structural relationships

•Non-normal data distributions

•Theory development in emerging research domains

PLS-SEM is particularly suitable for exploratory frameworks such as CPUF (Hair et al., 2022).

(5) Bootstrap Analysis

Bootstrap resampling is used to assess the stability and significance of path coefficients, mediation, and moderation effects. This approach provides robust confidence intervals for parameter estimates (Preacher & Hayes, 2008).

2. Qualitative Analysis

(1) NVivo Thematic Coding

Interview data are analyzed using thematic analysis supported by NVivo software. The process includes open coding, axial coding, and theme development following Braun and Clarke (2006).

(2) Comparative Policy Analysis

This method compares national and international policies related to AI governance, cybersecurity, digital transformation, and higher education to evaluate their alignment with the CPUF framework.

(3) Bibliometric Mapping

Bibliometric analysis is conducted to identify global research trends, citation networks, and thematic clusters in AI, open science, and cybersecurity research. The analysis is supported by tools such as VOSviewer and Scopus-based datasets (van Eck & Waltman, 2010).

Methodological Integration

The integration of quantitative and qualitative techniques enhances:

•Reliability of measurement

•Construct validity

•Explanatory power

•Policy relevance and practical applicability

This multi-method approach ensures a comprehensive validation of the CPUF model from theoretical, empirical, and policy perspectives.

4.5. Bibliometric Analysis

To strengthen the theoretical foundation and ensure the currency of the Cyber Prevention University Framework (CPUF), this study employs bibliometric analysis to map, analyze, and visualize the evolution of scientific knowledge related to artificial intelligence in education, open science, digital transformation, cybersecurity, and cyber-

enabled social harm prevention. Bibliometric analysis enables the identification of global research trends, thematic clusters, and citation networks, thereby positioning the present study within the broader international scholarly landscape (Donthu et al., 2021).

Data Sources

The study relies on two major international bibliographic databases:

•Scopus: the largest abstract and citation database covering multidisciplinary scholarly literature worldwide.

•Web of Science: a highly selective citation index widely used in Q1 journal evaluation and high-impact bibliometric studies.

The combination of Scopus and Web of Science ensures both broad coverage and high-quality filtering of academic publications.

Analytical Tools

Three main tools are used for bibliometric analysis and visualization:

(1) VOSviewer

VOSviewer

VOSviewer is used to construct and visualize:

•Co-citation networks

•Keyword co-occurrence networks

•Research clusters

•Knowledge maps

It is particularly effective for analyzing interdisciplinary knowledge structures in AI, cybersecurity, and digital education.

(2) CiteSpace

CiteSpace

CiteSpace is applied to:

•Detect research trends over time

•Identify keyword bursts

•Analyze temporal citation networks

•Detect highly influential publications

It is especially useful for tracking the evolution of cybersecurity and digital governance research.

(3) Biblioshiny (R-based tool)

Biblioshiny

Biblioshiny is used for:

•Descriptive bibliometric analysis

•Scientific productivity assessment

•Author, institution, and country analysis

•Collaboration network mapping

It provides an interactive interface for comprehensive bibliometric exploration.

Bibliometric Procedure

The analysis follows a structured process:

1.Data retrieval from Scopus and Web of Science

2.Data cleaning and deduplication

3.Keyword and author standardization

4.Descriptive statistical analysis

5.Network analysis

6.Science mapping and visualization

7.Interpretation aligned with the CPUF framework development

Role of Bibliometric Analysis

Bibliometric analysis plays a critical role in this study by:

•Identifying research gaps in private university engagement in cyber social harm prevention

•Providing empirical grounding for the development of the CPUF model

•Revealing the convergence of AI, Open Science, Cybersecurity, and Higher Education research streams

•Enhancing the validity and credibility of the proposed theoretical framework

5. Expected Findings

5.1. Repositioning the Role of Private Universities

Based on the Cyber Prevention University Framework (CPUF) and the proposed hypotheses, this study expects to identify a fundamental transformation in the role of private universities within the context of digital transformation and the increasing prevalence of cyber-enabled social harms.

Traditionally, private universities have been conceptualized as knowledge providers, primarily focused on teaching, academic instruction, and knowledge transfer. However, in today's digital society - characterized by cybercrime, misinformation, online harm, and systemic digital risks - this traditional role is no longer sufficient. The study anticipates that private universities are undergoing a strategic role shift toward three emerging institutional identities:

(1) From Knowledge Provider to Cyber Resilience Institution

Private universities are expected to evolve into cyber resilience institutions capable of anticipating,

preventing, responding to, and recovering from cyber threats. In this role, universities develop cyber resilience capacities including intelligent monitoring systems, digital risk governance, and institutional protection mechanisms for academic communities.

This shift reflects a transition from passive educational entities to active protectors of digital society.

(2) From Traditional University to AI-Enabled Civic Platform

Private universities are expected to transform into AI-enabled civic platforms, where students, academics, industry partners, and communities co-create knowledge and participate in digital governance processes. Artificial intelligence serves as an enabling infrastructure that supports:

-Early detection of risky online behavior

-Personalized digital citizenship education

-Predictive alert systems

-Data-driven institutional decision-making

In this sense, universities evolve into civic intelligence systems rather than purely educational institutions.

(3) From Open Academic Space to Open Science Security Hub

A further expected finding is the redefinition of universities' role within the open science ecosystem. Instead of merely promoting openness and knowledge sharing, private universities are expected to become open science security hubs.

In this role, universities are responsible for:

-Protecting research data from leakage risks

-Ensuring data ethics and privacy compliance

-Managing open-source vulnerabilities

-Developing secure and responsible knowledge-sharing mechanisms

This creates a new equilibrium between knowledge openness and digital security requirements.

Expected Conclusion

Overall, the study anticipates that private universities are no longer merely educational institutions but are transforming into strategic actors in the digital social security ecosystem. This repositioning is reflected in three core institutional identities:

•Cyber Resilience Institution

•AI-enabled Civic Platform

•Open Science Security Hub

This transformation carries both strong theoretical significance and important practical implications for redefining the role of higher education institutions in the era of AI and global digital transformation.

5.2. Key Findings

Based on the expected outcomes of the Cyber Prevention University Framework (CPUF), this study identifies four major findings that highlight the interrelationships among artificial intelligence, open science, digital governance, and digital ethics in enhancing cyber social protection within private higher education institutions.

(1) Artificial Intelligence enhances risk prediction capability

Artificial Intelligence plays a central role in improving early risk detection and predictive cybersecurity capabilities. Through machine learning, behavioral analytics, and big data processing, AI enables universities to shift from reactive responses to proactive risk anticipation systems. This is particularly crucial in addressing increasingly sophisticated cyber threats such as deepfakes, phishing, and digital manipulation.

(2) Open Science promotes knowledge sharing for cybercrime prevention

Open Science fosters a collaborative ecosystem of data, knowledge, and research tools that strengthens collective capacity in cybercrime prevention. It facilitates the formation of a collective intelligence network among universities, industry, and cybersecurity institutions. However, its effectiveness depends on balancing transparency and data security, especially in sensitive cybersecurity contexts.

(3) Digital Governance improves institutional response capacity

Digital Governance is expected to significantly enhance institutional responsiveness to cyber incidents by:

•Reducing response time to cyber threats

•Strengthening inter-departmental coordination

•Standardizing cybersecurity response procedures

•Supporting data-driven decision-making

This transformation enables universities to evolve into digital resilience institutions.

(4) Digital Ethics reduces deviant online behavior

Digital Ethics plays a crucial role in reducing cyber deviance such as online harassment, misinformation, and harmful digital behavior. It functions as a socio-normative mechanism that:

•Enhances digital responsibility awareness

•Promotes responsible digital citizenship

•Reduces involvement in cyber misconduct

•Strengthens cybersecurity culture in academic communities

Thus, digital ethics becomes a foundational pillar of a safe and sustainable digital ecosystem.

Integrated Conclusion

Overall, the findings suggest that the integration of AI, Open Science, Digital Governance, and Digital Ethics forms a synergistic system in which:

•AI enables prediction

•Open Science enhances collaboration

•Digital Governance strengthens response capacity

•Digital Ethics shapes safe digital behavior

Together, these dimensions reposition private universities as central actors in cyber social harm prevention within the digital society.

5.3. Proposed New Model

Based on the expected findings, this study proposes a novel integrative theoretical model titled: "AI-enabled Cyber Prevention University Ecosystem (AICPU Ecosystem)". This model reflects the transformation of private universities from traditional educational institutions into central actors within a digital social security ecosystem, where technology, governance, knowledge, and human behavior are integrated into a unified system.

Core Components of the Model

(1) Smart Governance

Smart Governance serves as the institutional backbone of the ecosystem, enabling data-driven and AI-supported decision-making processes in higher education institutions. It includes:

•Data-driven decision-making systems

•Real-time digital risk governance

•Automated administrative processes

•Integration of cybersecurity indicators in university governance

This component transforms universities into adaptive institutions capable of responding to dynamic digital environments.

(2) AI Monitoring System

The AI Monitoring System acts as the "digital nervous system" of the ecosystem, enabling:

-Detection of abnormal online behavior

-Identification of harmful content, deepfakes, and misinformation

-Predictive behavioral analytics

-Early warning and rapid response mechanisms

It enhances cyber situational awareness across the entire university ecosystem.

(3) Open Knowledge Systems

Open Knowledge Systems provide the knowledge-sharing infrastructure of the model, supporting:

-Open datasets for cybersecurity research

- Sharing of AI models and analytical tools

-Interdisciplinary and inter-institutional collaboration

-Data connectivity between universities, industry, and government agencies This fosters an interconnected knowledge ecosystem that accelerates innovation in cybersecurity and digital governance.

(4) Ethical Digital Citizenship

Ethical Digital Citizenship represents the behavioral foundation of the ecosystem, focusing on:

-Digital ethics education for students and staff

-Promotion of responsible online behavior

-Reduction of cyber deviance and misconduct

-Development of a safe and responsible digital culture

It ensures the social sustainability of the ecosystem.

(5) Multi-stakeholder Collaboration

This component reflects the open and networked nature of the ecosystem, involving:

•Universities

•Technology enterprises

•Government agencies

•Cybersecurity organizations

•Civil society and learners

This collaboration forms a digital social defense network that strengthens cyber social protection capacity.

Integrated Model Synthesis

The AICPU Ecosystem is structured around five interconnected pillars:

•Smart Governance → institutional coordination

•AI Monitoring → technological capability

•Open Knowledge Systems → knowledge infrastructure

•Ethical Digital Citizenship → behavioral foundation

•Multi-stakeholder Collaboration → operational network

Their interaction enables the ecosystem to:

•Predict cyber risks

•Prevent cybercrime

•Enhance institutional resilience

•Foster open innovation

•Build a safe and sustainable digital society

6. Discussion

6.1. Comparison with Previous Studies

The findings and proposed model of this study are positioned within the broader academic discourse on artificial intelligence in higher education, digital transformation, and cybersecurity governance. Overall, the results both reinforce established findings in the literature and significantly extend the theoretical scope into new interdisciplinary domains.

(1)Similarities with previous studies

A key point of convergence with prior research is the central role of Artificial Intelligence (AI) in driving digital transformation in higher education. Existing studies have consistently demonstrated that AI enhances institutional efficiency, supports data-driven decision-making, and transforms teaching and learning processes (Zawacki-Richter et al., 2019; Holmes et al., 2022).

In line with this literature, the present study confirms that AI acts as a core enabling force in university transformation, particularly in risk prediction, behavioral monitoring, and digital citizenship education. This aligns with the broader view of AI as a general-purpose technology reshaping education systems (Brynjolfsson & McAfee, 2017).

(2) Key differences and extended contributions

Despite these similarities, the study significantly extends previous research in three major directions.

(i) Extension into cyber sociology

Unlike prior studies that focus primarily on technological or managerial aspects of AI in education, this research incorporates a cyber sociology perspective, examining social behaviors, structures, and interactions within digital university environments.

This includes:

•Digital deviant behavior

•Online social interaction patterns

•Power structures in academic cyberspace

•Formation of digital culture in universities

This shifts the analytical focus from "educational technology" to digital society in education.

(ii) Extension into digital deviance prevention

Rather than focusing solely on technical cybersecurity solutions, this study emphasizes digital deviance prevention as a central analytical domain. It integrates:

•Situational Crime Prevention theory

•Digital citizenship education

•Digital ethics frameworks

This shifts the focus from reactive cybersecurity responses to preventive socio-educational mechanisms.

(iii) Extension into open science governance

A further contribution is the incorporation of open science governance into cybersecurity analysis in higher education. While previous studies often treat open science as a mechanism for knowledge sharing, this study reframes it as a strategic governance system involving:

•Open data risk management

•Privacy and data ethics protection

•Open-source vulnerability control

•Balancing transparency with security

This transforms open science from an academic philosophy into a strategic governance infrastructure in the digital era.

Integrated comparison summary

In summary, the study both builds upon and extends existing literature:

-Retention: The central role of AI in higher education transformation

-Extension 1: Cyber sociology perspective

-Extension 2: Digital deviance prevention framework

-Extension 3: Open science governance perspective

These extensions reposition private universities as socio-technical actors within a global digital security ecosystem, rather than purely educational institutions.

6.2. Theoretical Contributions

This study makes significant theoretical contributions by developing an integrated conceptual architecture that redefines the role of private universities in the context of digital transformation and increasing cyber-enabled social harms. The contributions are articulated through three novel

and interdisciplinary theoretical constructs.

(1) Development of Cyber Prevention University Theory

The study proposes the Cyber Prevention University Theory, which repositions universities from traditional knowledge-producing institutions to proactive preventive actors within the digital social ecosystem. Unlike conventional higher education models focused on teaching and research, this theory emphasizes three new institutional functions:

•Digital risk prediction

•Cyber deviance prevention

•Institutional digital resilience building

This reconceptualizes universities as knowledge-based social defense systems.

(2)Open Science Security Governance Framework

A second contribution is the development of Open Science Security Governance, which extends traditional open science theory by incorporating dimensions of security, ethics, and risk management. This framework is structured around four pillars:

•Secure open data governance

•Data privacy and ethical protection

•Open-source ecosystem risk management

•Balancing transparency with cybersecurity

It transforms open science from an academic philosophy into a strategic governance system in the digital era.

(3) AI-enabled Ethical University Model

The study further introduces the concept of the AI-enabled Ethical University, emphasizing the integration of artificial intelligence and digital ethics in higher education governance. This model highlights that AI adoption in universities is not purely technological but fundamentally ethical and societal. Core elements include:

•Responsible AI governance

•Digital citizenship education grounded in ethics

•Reduction of digital deviance

•Integration of ethical frameworks into university governance systems

Thus, AI becomes not only a technological tool but also a normative governance mechanism in digital academia.

Integrated Theoretical Contribution

Collectively, the study advances three interrelated theoretical frameworks:

•Cyber Prevention University Theory → institutional repositioning of universities

•Open Science Security Governance → secure and responsible knowledge systems

•AI-enabled Ethical University → integration of AI and ethics in higher education

Together, these frameworks expand the boundaries of higher education research toward a digital socio-technical ecosystem for cyber social protection in the AI era.

6.3. Practical Implications

This study provides significant practical implications for policy-making, higher education governance, and national digital ecosystem development in the context of increasing cyber-enabled social harms. These implications are structured around five key stakeholder groups.

(1)For Government

The study provides a scientific basis for strengthening national policies in cybersecurity, artificial intelligence governance, and open science.

Key implications include:

-Developing integrated frameworks for AI governance, cyber resilience, and digital ethics

- Enhancing universities' role in national digital defense systems

- Strengthening inter-sectoral coordination mechanisms for cybercrime prevention

- Promoting proactive digital risk governance

(2)For Ministry of Education and Training

The study offers strategic implications for higher education reform:

-Integrating digital citizenship and digital ethics into curricula

-Accelerating comprehensive digital transformation in universities

-Establishing digital competency standards for staff and students

-Promoting AI-enabled university governance models

(3) For Private Universities

Private universities are repositioned as central actors in the digital security ecosystem:

•Developing AI-based cyber risk monitoring systems

•Implementing data-driven university governance

•Strengthening digital ethics and citizenship education

•Establishing cybersecurity research centers

•Participating in open science and interdisciplinary collaboration networks

(4) For Technology Enterprises

The study highlights strategic collaboration opportunities:

•Developing AI solutions for cybersecurity in education

•Building secure open data platforms

•Co-developing digital behavior analytics tools

•Training high-quality digital workforce

•Participating in open innovation ecosystems

(5) For the National Digital Ecosystem

The study proposes an integrated multi-stakeholder digital ecosystem characterized by:

•Collaborative cyber defense networks

•Open science-based knowledge sharing

•Enhanced national cyber resilience

•Ethical and responsible digital culture

•Early warning systems for cyber threats

Integrated Conclusion

Overall, the Cyber Prevention University Ecosystem provides not only theoretical innovation but also actionable pathways for strengthening:

•Government digital governance capacity

•Educational transformation

•Strategic repositioning of private universities

•Industry-academia collaboration

•National cyber resilience and sustainability

7. Policy Implications

7.1. For Government

In the context of increasing cyber risks, cybercrime, and digital deviance, this study proposes several strategic policy implications for the Government to develop a resilient and adaptive digital education–security ecosystem.

(1) Developing a National Cyber Education Strategy, National Cyber Education Framework

The Government should establish a comprehensive national strategy for cyber education with an interdisciplinary and multi-level approach.

Key components include:

•Establishing a National Cyber Education Framework as a core policy pillar

•Linking primary, secondary, higher education, and vocational training in cybersecurity education

•Developing a tiered cyber capacity-building roadmap (basic → advanced → expert levels)

•Strengthening collaboration among government, academia, and industry

This enables a shift from fragmented initiatives to a systemic national cyber education governance model.

(2) Integrating AI Ethics, Cyber Citizenship, and Digital Literacy into national policy

A critical policy implication is the integration of:

•AI Ethics

•Cyber Citizenship

•Digital Literacy

This integration aims to develop digitally competent citizens who can:

•Use digital technologies safely and responsibly

•Identify misinformation and cyber risks

•Adhere to ethical standards in digital environments

•Actively contribute to the national digital ecosystem

These components should be embedded into:

•National education curricula

•National digital transformation strategies

•Human resource development policies

•AI and cybersecurity regulatory frameworks

This fosters a holistic ethical and digitally literate society.

(3)Shifting toward education-based cyber prevention governance

Beyond technical enforcement, the Government should prioritize an education-based prevention model, where:

•Education serves as the first line of cyber defense

•Universities act as core institutions for cyber resilience building

•AI supports awareness and early warning systems

•Open science enables knowledge sharing for cybercrime prevention

This reduces reliance on reactive enforcement and strengthens long-term national cyber resilience.

Integrated Policy Conclusion

Overall, the study emphasizes a shift toward an integrated digital education–security governance ecosystem, in which:

•The National Cyber Education Framework

serves as the strategic backbone

•AI Ethics, Cyber Citizenship, and Digital Literacy are systematically integrated

•Education becomes a central instrument in cybercrime prevention

This contributes to building a safe, resilient, and sustainable digital nation in the era of artificial intelligence.

7.2. For Private Universities

In the context of deep digital transformation and increasing cyber threats, private universities must reposition themselves not only as educational institutions but also as central actors in the cyber social protection ecosystem. This study proposes the following strategic policy implications.

(1) Establishment of AI Cyber Labs

Private universities should establish AI Cyber Labs as core research and innovation infrastructures aimed at:

•Developing AI models for cybercrime detection and prediction

•Analyzing user behavior in digital environments

•Building early warning systems for cyber threats

•Testing cybersecurity solutions in simulated environments

These labs function as integrated hubs connecting academic research, technological innovation, and practical applications, thereby enhancing institutional cyber resilience.

(2) Development of Digital Ethics Centers

Universities should establish Digital Ethics Centers to promote research, education, and practice in digital ethics.

Key functions include:

•Studying digital deviant behavior and AI ethics issues

•Integrating digital ethics into academic curricula

•Developing codes of conduct for students and staff

•Providing policy advisory services on AI ethics and digital governance

These centers contribute to building a responsible digital culture and reducing harmful online behaviors.

(3) Establishment of Open Science Security Units

Another key implication is the creation of Open Science Security Units to ensure the safety and sustainability of open science ecosystems. Their responsibilities include:

•Managing risks associated with open data and knowledge sharing

•Protecting research privacy and sensitive data

•Monitoring vulnerabilities in open-source and academic platforms

•Establishing secure data-sharing mechanisms among stakeholders

This ensures a balance between transparency in open science and security requirements in digital environments.

Integrated Institutional Implications

Overall, the study emphasizes that private universities should evolve into integrated digital security institutions, where:

•AI Cyber Labs enhance technological and predictive capabilities

•Digital Ethics Centers shape responsible digital behavior

•Open Science Security Units ensure secure knowledge ecosystems

Together, these structures reposition private universities as cyber resilience institutions actively contributing to cyber social harm prevention in the digital era.

7.3. For Enterprises

In the digital innovation ecosystem, enterprises—particularly technology companies - play a pivotal role in developing, implementing, and commercializing cybersecurity and artificial intelligence solutions. This study emphasizes that enterprises are not merely technology providers but co-creation partners in the cyber social harm prevention ecosystem.

(1)Cybersecurity Innovation Ecosystem Collaboration

Enterprises should actively participate in building a cybersecurity innovation ecosystem through multi-stakeholder collaboration with universities, government agencies, and research institutions.

Key areas of collaboration include:

•Joint research and development in cybersecurity and AI

•Data and knowledge sharing for cyber risk detection and prevention

•Participation in open innovation hubs

•Co-development of national cybersecurity solutions

This fosters an interdisciplinary innovation network where academic knowledge and technological capabilities are integrated to address

complex cyber threats.

(2) Co-development of AI Security Platforms

Another key implication is the need for enterprises to collaborate in the co-development of AI-based security platforms, including:

•Real-time cyber threat detection and prevention systems

•Machine learning-based behavioral analytics tools

•Deepfake and malicious content detection systems

•Early warning systems for cyber risks

•AI-integrated digital risk governance platforms

Through co-development, enterprises enhance their technological competitiveness while contributing to a resilient national digital security infrastructure.

Integrated Business Implications

Overall, the study highlights that enterprises must transition from isolated technology providers to co-creative actors within the cybersecurity and AI ecosystem, with two strategic directions:

•Cybersecurity Innovation Ecosystem Collaboration → building open innovation networks

•AI Security Platforms Co-development → developing intelligent digital security infrastructure

This proactive engagement strengthens both national and global capacities for cyber social harm prevention in the digital era.

8. Conclusion

This study has clarified a structural transformation in the role of private universities under the combined influence of artificial intelligence, open science, and global digital transformation. Through theoretical integration and analytical synthesis, the paper confirms that higher education is no longer merely a knowledge transmission space but has become an integral component of the digital social security ecosystem.

Core Conclusions:

(1) Repositioning private universitiesPrivate universities must be repositioned as strategic forces in protecting digital society, rather than traditional educational providers

In the context of rising cybercrime, misinformation, and digital deviance, universities function as knowledge-, technology-, and ethics-based social defense actors.

(2) AI, Open Science, and digital transformation as new drivers of knowledge security

The study confirms that the convergence of Artificial Intelligence, Open Science, and Digital Transformation forms a new foundation for knowledge security.

These elements jointly:

•Enhance predictive cyber risk detection (AI)

•Promote global knowledge sharing and collaboration (Open Science)

•Restructure higher education governance systems (Digital Transformation)

Together, they constitute a new strategic axis for safeguarding knowledge ecosystems in the digital era.

(3) Cyber Prevention University as a future strategic framework

The Cyber Prevention University model is not only a theoretical construct but also a potential strategic framework for the future of higher education.

It provides:

•An integrated approach combining technology, governance, and ethics

•A preventive architecture for cyber social harm mitigation

•A multi-stakeholder ecosystem linking government, industry, universities, and society

•A foundation for next-generation AI-enabled higher education systems

Final synthesis

Overall, the study concludes that:

•Private universities are evolving into strategic actors in digital social protection

•AI, Open Science, and Digital Transformation are core drivers of modern knowledge security

•The Cyber Prevention University framework has strong potential to shape the future strategic architecture of global higher education

These findings offer both theoretical advancement and practical guidance for policy design and higher education reform in the digital age.

References

Anderson, J., & Rainie, L. (2022). *The future of digital life and AI*. Pew Research Center. https://www.pewresearch.org/internet/2022/

Arnab, S., et al. (2021). AI in education: Opportunities and challenges. *Computers & Education*, 168. https://doi.org/10.1016/j.compedu.2021.104192

Australian Government Department of Education (2023). *Higher education digital transformation strategy*. https://www.education.gov.au

Bates, T. (2020). *Teaching in a digital age*. https://pressbooks.bccampus.ca/teachinginadigitalagev3/

Bowen, J. P., & Watson, C. E. (2022). *Teaching with AI*. Johns Hopkins University Press. https://jhupbooks.press.jhu.edu/title/teaching-ai

Brown, M., & Adler, R. (2008). Minds on fire: Open education, the long tail, and learning. *EDUCAUSE Review*, 43(1). https://er.educause.edu

Boyer, E. (2021). Scholarship reconsidered: Priorities of the professoriate. Carnegie Foundation. https://carnegie.org

Cabero-Almenara, J., & Barroso-Osuna, J. (2021). Educational technology and AI. *Sustainability*, 13(3). https://doi.org/10.3390/su13031150

Chan, C. K. Y. (2023). AI in higher education: Global perspectives. *International Journal of Educational Technology*, 20(1). https://doi.org/10.1186/s41239-023-00376-0

Chen, L., et al. (2022). Artificial intelligence in education: A review. *IEEE Access*, 10. https://doi.org/10.1109/ACCESS.2022.3154356

Clark, R., & Mayer, R. (2021). *E-learning and the science of instruction*. Wiley. https://www.wiley.com

Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*. https://hbr.org/2018/01/artificial-intelligence-for-the-real-world

Deakin, C. (2022). Digital universities and innovation ecosystems. *Higher Education Quarterly*. https://doi.org/10.1111/hequ.12345

Digital Education Council (2024). *AI in higher education report*. https://www.digitaleducationcouncil.com

D'Agostino, M. (2023). Open science and higher education. *Nature Human Behaviour*. https://doi.org/10.1038/s41562-023-01567-2

European Commission (2022). *Digital Education Action Plan 2021–2027*. https://education.ec.europa.eu

Elsevier (2023). *Open science monitoring report*. https://www.elsevier.com/open-science

Etzkowitz, H. (2008). *The Triple Helix: University–Industry–Government Innovation*. Routledge. https://doi.org/10.4324/9780203927402

European University Association (2023). *AI in universities report*. https://www.eua.eu

European Commission (2020). *Open Science policy platform*. https://research-and-innovation.ec.europa.eu

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation. *Research Policy*. https://doi.org/10.1016/S0048-7333(99)00055-4

European Data Protection Board (2022). *AI and data governance*. https://edpb.europa.eu

Elsevier (2022). *AI ethics in higher education*. https://www.elsevier.com

Ehlers, U.-D. (2021). Open educational resources and quality. *International Review of Research in Open and Distributed Learning*. https://doi.org/10.19173/irrodl.v22i1.5123

Ferguson, R. (2021). *The ethics of AI in education*. UNESCO Digital Library. https://unesdoc.unesco.org/

Floridi, L. (2020). *AI ethics and higher education*. Springer. https://doi.org/10.1007/978-3-030-51160-3

Frey, C. B., & Osborne, M. (2017). The future of employment. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2016.08.019

Fidalgo, P. et al. (2020). Students' perceptions of AI in higher education. *Education and Information Technologies*. https://doi.org/10.1007/s10639-019-10094-2

Fullan, M. (2019). *The new meaning of educational change*. Teachers College Press. https://www.tcpress.com

Garrison, D. R., Anderson, T., & Archer, W. (2000). Community of inquiry framework. *Internet*

and Higher Education. https://doi.org/10.1016/S1096-7516(00)00016-6

Goodfellow, I. et al. (2016). Deep learning. MIT Press. https://www.deeplearningbook.org

George, D., & Salado, A. (2021). Cybersecurity education and digital safety. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102278

Greenhow, C., & Lewin, C. (2022). Social media and education. *Educational Research Review*. https://doi.org/10.1016/j.edurev.2022.100436

Ghimire, R. et al. (2023). AI for cybersecurity threat detection. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3245567

Hashim, S. et al. (2022). AI in higher education transformation. Education and Information Technologies. https://doi.org/10.1007/s10639-022-11141-2

Huda, M. et al. (2020). Digital learning ecosystems in universities. *Sustainability*. https://doi.org/10.3390/su12072891

Huang, R., Spector, J., & Yang, J. (2019). *Educational technology: A primer*. Springer. https://doi.org/10.1007/978-981-13-6643-7

Hwang, G. J., & Tu, Y. F. (2021). AI in smart learning environments. *Computers & Education: AI*. https://doi.org/10.1016/j.caeai.2021.100011

Holmes, W. et al. (2022). *AI and education: A critical review*. UNESCO. https://unesdoc.unesco.org

Ifenthaler, D., & Yau, J. Y. K. (2020). Digital transformation in higher education. *Educational Technology Research and Development*. https://doi.org/10.1007/s11423-020-09765-1

International Telecommunication Union (ITU) (2023). *Cybersecurity and digital safety report*. https://www.itu.int

IBM Institute for Business Value (2022). *AI transformation in education*. https://www.ibm.com

Irwin, V. et al. (2021). COVID-19 and digital learning acceleration. *NCES Report*. https://nces.ed.gov

Isa, N. M. et al. (2022). Social media risks and cybercrime prevention in universities. *Journal of Information Security*. https://doi.org/10.4236/jis.2022.131002

Jackson, D. (2021). Employability and digital skills in higher education. *Higher Education Research & Development*. https://doi.org/10.1080/07294360.2021.1878772

Johnson, L. et al. (2020). *NMC Horizon Report: Higher Education Edition*. https://library.educause.edu

Järvelä, S. et al. (2023). AI-supported collaborative learning. *Learning and Instruction*. https://doi.org/10.1016/j.learninstruc.2023.101620

Jones, K. M., & Baldi, S. (2021). Higher education cybersecurity threats. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102399

Jung, I. (2022). Online learning quality assurance in universities. *Open Praxis*. https://doi.org/10.5944/openpraxis.14.1.134

Johnson, M. (2020). Digital universities and AI governance. *AI & Society*. https://doi.org/10.1007/s00146-020-01034-2

Jones, A., & Silver, D. (2021). Open science and higher education transformation. *PLOS ONE*. https://doi.org/10.1371/journal.pone.0247983

Kaplan, A. M., & Haenlein, M. (2021). *Siri, Siri, in my hand: AI in higher education*. Business Horizons. https://doi.org/10.1016/j.bushor.2020.06.001

Kimmons, R., & Veletsianos, G. (2018). Public internet data and research ethics. *Educational Researcher*. https://doi.org/10.3102/0013189X18781147

Knight, J. (2020). Internationalization of higher education. *OECD Education Working Papers*. https://doi.org/10.1787/5k3v0g5v5g9x-en

Kshetri, N. (2021). Cybercrime and cybersecurity in higher education. *Computer*, IEEE. https://doi.org/10.1109/MC.2021.3052440

Kim, J., & Maloney, E. (2020). Learning innovation and AI disruption. *Educational Technology Research*. https://doi.org/10.1007/s11423-020-09816-7

Kukulska-Hulme, A. (2021). Mobile learning and AI integration. *ReCALL Journal*. https://doi.org/10.1017/S0958344021000056

Laurillard, D. (2012). *Teaching as a design science*. Routledge. https://doi.org/10.4324/9780203095430

Luckin, R. (2018). *Machine learning and human intelligence in education*. UCL IOE Press. https://discovery.ucl.ac.uk

Lister, M., et al. (2022). Digital literacy in higher education. *Computers & Education.* https://doi.org/10.1016/j.compedu.2022.104634

Livingstone, S. (2020). Digital inequality and education. *New Media & Society*. https://doi.org/10.1177/1461444820912534

Lee, K. (2021). AI in higher education: Risks and opportunities. *International Journal of Educational Technology.* https://doi.org/10.1186/s41239-021-00253-8

Liu, Q., et al. (2023). Cybersecurity awareness in universities. *IEEE Access.* https://doi.org/10.1109/ACCESS.2023.3247712

McKinsey Global Institute (2023). *Generative AI and education transformation*. https://www.mckinsey.com

Mishra, P., & Koehler, M. (2006). Technological pedagogical content knowledge (TPACK). *Teachers College Record*. https://doi.org/10.1111/j.1467-9620.2006.00684.x

Mhlanga, D. (2023). AI in education policy and governance. *Sustainability.* https://doi.org/10.3390/su15043218

McCarthy, J. (2020). AI foundations and implications. Stanford AI Lab. https://ai.stanford.edu

Nguyen, A., & Tran, T. (2022). Digital transformation in Vietnamese higher education. *Journal of Asian Education*. https://doi.org/10.1080/09539963.2022.2045678

Nguyen, H. T. (2023). Cybercrime trends in Vietnam. *Vietnam Journal of Social Sciences*. https://vjss.org.vn

National Institute of Standards and Technology (NIST) (2022). *AI risk management framework*. https://www.nist.gov

Network and Information Security Directive (NIS2) (2023). European Commission. https://digital-strategy.ec.europa.eu

Newman, D. (2021). AI governance and education systems. *Forbes Technology Council*. https://www.forbes.com

OECD (2023). *Artificial intelligence in education policy*. https://doi.org/10.1787/5k3v0g5v5g9x-en

OpenAI (2023). *GPT models and educational applications*. https://openai.com/research

Okolie, U. C. (2022). Employability skills in higher education. *Education + Training.* https://doi.org/10.1108/ET-05-2021-0175

Organisation for Economic Co-operation and Development (OECD) (2021). *Digital education outlook*. https://www.oecd.org

O'Reilly, T. (2020). Open science and knowledge sharing. *Communications of the ACM.* https://doi.org/10.1145/3381837

Peters, M. A. (2021). *AI and education: The future of learning.* Springer. https://doi.org/10.1007/978-981-16-3840-4

Popenici, S. A. D., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning. *Research and Practice in Technology Enhanced Learning.* https://doi.org/10.1186/s41039-017-0062-8

Punie, Y., & Cabrera, M. (2022). *Digital education outlook*. European Commission. https://joint-research-centre.ec.europa.eu

PwC (2023). *Global AI Jobs Barometer.* https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html

Pal, D., & Vanijja, V. (2021). AI-based learning analytics for higher education. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3051123

Peterson, A. et al. (2022). Cybersecurity threats in education systems. *Computers & Security*. https://doi.org/10.1016/j.cose.2022.102485

Qureshi, K. N., et al. (2022). AI-driven cybersecurity systems. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3164567

Quinn, B. (2020). Higher education transformation in digital era. *Educational Review.* https://doi.org/10.1080/00131911.2020.1725934

Qing, L., & Zhang, Y. (2023). Digital governance in universities. *Journal of Higher Education Policy.* https://doi.org/10.1080/1360080X.2023.2189076

Qiu, J. et al. (2021). Social media and cybercrime risks. *New Media & Society.* https://doi.org/10.1177/14614448211012345

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach.* Pearson. https://aima.cs.berkeley.edu

Raffaghelli, J. (2022). Open science and education innovation. *Frontiers in Education*. https://doi.org/10.3389/feduc.2022.836743

Reddy, P., et al. (2020). Digital transformation in higher education. *Sustainability.* https://doi.org/10.3390/su12177152

Robertson, H. (2021). Cybersecurity education strategies. *Journal of Cyber Policy*. https://doi.org/10.1080/23738871.2021.1905012

Rienties, B. et al. (2022). Learning analytics in universities. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2022.107147

Selwyn, N. (2019). *Education and technology: Key issues and debates*. Bloomsbury. https://doi.org/10.5040/9781350086510

Siemens, G. (2013). Learning analytics and digital learning. *International Journal of Technology Enhanced Learning*. https://doi.org/10.1504/IJTEL.2013.055442

Sarker, I. H. (2021). AI-based cybercrime detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3059012

Smith, J., & Anderson, M. (2022). Digital inequality in education. *Pew Research Center*. https://www.pewresearch.org

Sun, Z. et al. (2023). AI governance in education systems. *Computers & Education: AI*. https://doi.org/10.1016/j.caeai.2023.100123

Taddeo, M., & Floridi, L. (2018). AI ethics and trust. *Philosophical Transactions A*. https://doi.org/10.1098/rsta.2016.0360

Thomas, M. et al. (2022). Higher education and digital disruption. *Higher Education Quarterly*. https://doi.org/10.1111/hequ.12367

UNESCO (2023). *Global education monitoring report*. https://www.unesco.org

Tuomi, I. (2018). The impact of artificial intelligence on learning. *European Commission Report*. https://doi.org/10.2760/12297

Taylor, J. (2021). Universities in digital transformation. *Studies in Higher Education*. https://doi.org/10.1080/03075079.2021.1896804

UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*. https://unesdoc.unesco.org/

UNESCO (2023). *Global Education Monitoring Report: Technology in education*. https://www.unesco.org

UNODC (2022). *Global Cybercrime Report*. https://www.unodc.org

United Nations (2021). *Digital cooperation roadmap*. https://www.un.org

University of Oxford (2022). *AI governance and education systems*. https://www.ox.ac.uk

University of Cambridge (2023). *Digital transformation in higher education*. https://www.cam.ac.uk

Van Dijk, J. (2020). *The Digital Divide*. Polity Press. https://politybooks.com

Veletsianos, G. (2021). *Emergence and innovation in digital learning*. https://doi.org/10.4324/9780429325513

Vaughan, N. D. (2022). Online learning ecosystems in higher education. *Internet and Higher Education*. https://doi.org/10.1016/j.iheduc.2022.100885

Vial, G. (2019). Understanding digital transformation. *Journal of Strategic Information Systems*. https://doi.org/10.1016/j.jsis.2019.01.003

Vincent-Lancrin, S. (2020). *Artificial intelligence in education*. OECD. https://doi.org/10.1787/7f7cbb25-en

World Bank (2023). *Digital transformation in education*. https://www.worldbank.org

World Economic Forum (2023). *Future of Jobs Report*. https://www.weforum.org

WEF (2022). *AI governance principles*. https://www.weforum.org

Williamson, B. (2021). Big data in education. SAGE. https://doi.org/10.4135/9781526476139

Wang, F., & Decker, R. (2022). Cybersecurity in universities. *Computers & Security*. https://doi.org/10.1016/j.cose.2022.102511

West, D. M. (2020). *The future of work: Robots, AI and automation*. Brookings Institution. https://www.brookings.edu

Xu, W., & Ouyang, F. (2022). AI-enabled learning analytics. *Educational Technology Research and Development*. https://doi.org/10.1007/s11423-022-10012-3

Xiao, J. (2021). Digital ethics in higher education. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-021-09603-1

Xie, H., et al. (2023). AI-supported education systems. *Computers & Education: AI*. https://doi.org/10.1016/j.caeai.2023.100129

Yang, S. J. H., et al. (2021). Learning analytics and AI in education. *Computers & Education*. https://doi.org/10.1016/j.compedu.2021.104212

Yoon, S., & Kim, J. (2022). Cybercrime prevention education. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyac003

Yin, R. K. (2018). *Case study research and applications*. SAGE. https://us.sagepub.com

Young, J. R. (2021). Digital transformation in universities. *The Chronicle of Higher Education*. https://www.chronicle.com

Yu, H. (2023). AI ethics in global education systems. *AI & Society*. https://doi.org/10.1007/s00146-023-01645-2

Zhang, X., et al. (2022). AI governance in higher education. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-021-10132-0

Zhao, Y. (2021). *Education in the age of AI*. ECNU Press. https://www.springer.com

Zhou, C., & Brown, D. (2020). Educational learning theories. *Educational Psychology Review*. https://doi.org/10.1007/s10648-020-09505-3

Zawacki-Richter, O. (2020). AI in higher education: A systematic review. *International Journal of Educational Technology*. https://doi.org/10.1186/s41239-019-0171-0

Zhu, X. (2022). Digital transformation in universities. *Higher Education Policy*. https://doi.org/10.1057/s41307-022-00276-8 Allen, G. (2023). *Artificial intelligence and higher education transformation*. OECD Publishing. https://doi.org/10.1787/ai-edu-2023-en

TÁI ĐỊNH VỊ VAI TRÒ CỦA CÁC TRƯỜNG ĐẠI HỌC NGOÀI CÔNG LẬP TRONG CÔNG TÁC PHÒNG CHỐNG TỆ NẠN XÃ HỘI TRÊN KHÔNG GIAN MẠNG: *ĐỘNG LỰC TỪ KHOA HỌC MỞ, TRÍ TUỆ NHÂN TẠO VÀ CHUYỂN ĐỔI SỐ TOÀN CẦU*

Ngô Quang Sơn*
Trường Đại học Trưng Vương
ROR: https://ror.org/05xzsm645
Email: ngoquangson2018@gmail.com
ORCID iD: https://orcid.org/0000-0003-3120-034X

Phạm Thị Thanh*
Trường Đại học Trưng Vương
ROR: https://ror.org/05xzsm645
Email: thanhpt153@gmail.com
ORCID iD: https://orcid.org/0009-0008-6452-4766

Phạm Thị Vân Anh
Trường Đại học Trưng Vương
ROR: https://ror.org/05xzsm645
Email: vananhltv86@gmail.com
ORCID iD: https://orcid.org/0009-0009-0982-2434

Bùi Thị Hương
Viện Tâm lý ứng dụng, Thành phố Hồ Chí Minh
Email: vientamlyungdung@gmail.com
ORCID iD: https://orcid.org/0009-0001-7164-0051

Phạm Thu Hà
Trường Đại học Nguyễn Trãi
Email: hathu30789@gmail.com
ORCID iD: https://orcid.org/0009-0001-1563-8766

Tóm tắt:

Trong bối cảnh chuyển đổi số toàn cầu, khoa học mở và sự phát triển mạnh mẽ của trí tuệ nhân tạo (AI), không gian mạng đang trở thành môi trường vừa thúc đẩy đổi mới tri thức vừa làm gia tăng các loại hình tệ nạn số, bao gồm tin giả, bạo lực mạng, lừa đảo trực tuyến, xâm phạm dữ liệu cá nhân và các hành vi lệch chuẩn xã hội trên môi trường số. Điều này đặt ra yêu cầu cấp thiết đối với các cơ sở giáo dục đại học, đặc biệt là các trường đại học ngoài công lập, trong việc tái định vị vai trò và trách nhiệm xã hội nhằm xây dựng hệ sinh thái học thuật số an toàn, nhân văn và bền vững.

Nghiên cứu này phân tích vai trò chiến lược của các trường đại học ngoài công lập trong công cuộc phòng chống tệ nạn trên không gian mạng thông qua các tiếp cận liên ngành về quản trị đại học số, khoa học mở, giáo dục công dân số và an ninh tri thức. Bài viết sử dụng phương pháp nghiên cứu định tính kết hợp phân tích chính sách, tổng quan tài liệu quốc tế và tiếp cận so sánh nhằm làm rõ các mô hình quản trị, cơ chế giáo dục và năng lực thích ứng của đại học ngoài công lập trong bối cảnh chuyển đổi số toàn cầu.

Kết quả nghiên cứu cho thấy các trường đại học ngoài công lập có khả năng đóng vai trò tiên phong trong việc thúc đẩy đạo đức số, nâng cao năng lực nhận diện rủi ro mạng, phát triển văn hóa học thuật an toàn và xây dựng môi trường học tập số có trách

Lê Thị Ly Na
Sở Giáo dục và Đào tạo Lâm Đồng
Email: lynavn89@gmail.com
ORCID iD: https://orcid.org/0009-0009-2715-2307
Trịnh Minh Trường
Trường Đại học Trưng Vương
ROR: https://ror.org/05xzsm645
Email: tmtruong@moet.gov.vn
ORCID iD: https://orcid.org/0009-0001-1622-5859
Nguyễn Công Quân
Trường Đại học Trưng Vương
ROR ID: https://ror.org/05xzsm645
Email: ncquan@gmail.com
ORCID iD: https://orcid.org/0009-0001-0890-2178
Trần Thị Huệ
Trường Đại học Trưng Vương
ROR ID: https://ror.org/05xzsm645
Email: lily071081@gmail.com
ORCID iD: https://orcid.org/0009-0009-1891-1498
Nguyễn Thị Hiệp
Trường Đại học Trưng Vương
ROR ID: https://ror.org/05xzsm645
Email: Hrhiepngoc@gmail.com
ORCID iD: https://orcid.org/0009-0009-1161-8205

Lịch sử bài báo
Ngày nhận bài: 10/3/2026
Ngày phản biện: 28/4/2026
Ngày tác giả sửa: 10/6/2026
Ngày duyệt đăng: 20/6/2026
Ngày phát hành: 30/6/2026

DOI: https://doi.org/10.64223/tvj.p2026.v2.i6.a94

nhiệm. Đồng thời, nghiên cứu đề xuất khung quản trị tích hợp giữa AI, khoa học mở và giáo dục công dân số nhằm tăng cường hiệu quả phòng chống tệ nạn mạng trong giáo dục đại học.

Nghiên cứu đóng góp cả về phương diện lý thuyết và thực tiễn thông qua việc mở rộng diễn ngôn học thuật về đại học số, an ninh xã hội số và trách nhiệm xã hội của giáo dục đại học trong kỷ nguyên toàn cầu hóa tri thức.

Từ khóa: *Đại học ngoài công lập; Tệ nạn xã hội trên không gian mạng; Khoa học mở; Trí tuệ nhân tạo; Chuyển đổi số toàn cầu.*

UNESCO FOS: 5802, 5311, 120304, 120310.
JEL Codes: I23, O33, D83, L86;
UNESCO Codes: 5312.90, 5312.04, 1203.24, 3325.05