

# Perceptions of Socio-Technological Shifts and Ethical Risks among Next-Generation Emirati IT Specialists: An Empirical Assessment

DIMITRIOS XANTHIDIS<sup>1</sup>, ANANG JUDAYA MUHAMAD AMIN<sup>1</sup>,  
OURANIA K. XANTHIDOU<sup>2</sup>, MOATAZ SALHAB<sup>1</sup>, ABDELRAHMAN ALTIGANI<sup>1</sup>,  
ALYA YOUSEF ABDULLA ALHAMMADI<sup>1</sup>

<sup>1</sup>Computer Information Sciences,  
Higher Colleges of Technology,  
Academic City - Dubai,  
UNITED ARAB EMIRATES

<sup>2</sup>Computer Science,  
Brunel University London,  
Kingston Ln, Uxbridge, UB8 3PH,  
UNITED KINGDOM

**Abstract:** - The accelerating evolution of digital infrastructures and cognitive technologies has fundamentally reshaped contemporary social fabrics; a complex matrix of systemic opportunities and ethical challenges. However, while the socio-economic dividends of automation abound, the swift and uncoordinated spread of these tools poses significant disruptions to traditional socio-cultural norms, ethical paradigms, and long-standing religious values. For highly advanced governmental and judicial technical frameworks in a rapidly growing economy like the United Arab Emirates, this digital transformation happens during a critical transition through legacy infrastructure disparities, often termed the digital divide, that exist in tandem with advanced governmental and judicial technical frameworks. While sophisticated solutions, including automation and artificial intelligence, such as intelligent legal informatics, predictive machine learning, and nuanced digital forensics, play a substantial role in optimizing security frameworks, compliance architectures, and compliance processes, they also introduce new sources of exploitation for automated bias, algorithmic manipulation, and the erasure of cryptographic evidence. At the same time, rampant deepfakes, organized disinformation schemes, and generative AI systems undermine trust, necessitating strict legal and operational scrutiny of content authenticity, platform accountability, and user cognitive health. This paper provides a systematic empirical analysis of next-generation Emirati IT professionals' levels of awareness about these sociotechnical vectors. Using an extensive questionnaire-level survey given to about 200 upper-level computer information sciences students, our initial empirical results suggest a rather sophisticated awareness baseline. The participants express considerable critical awareness of the structural, ethical, and socio-psychological dangers of these new paradigms and show a strong cultural and occupational capability to imaginatively think, govern, and steer future technologies responsibly.

**Key-Words:** - IT and Social Ethics, Sociotechnical Risk, Misinformation Frameworks, Deepfake Detection, Digital Inequity, Algorithmic Governance.

Received: February 7, 2026. Revised: April 15, 2026. Accepted: June 18, 2026. Published: October 7, 2026.

## 1 Introduction

The speed at which technology is progressing so rapidly now is no longer simply a matter of operational efficiency, but is now also a vital socio-political engine driving powerful structural conditions, social transactions and religious observances. The macroeconomic and systemic benefits of digital transformation are well-documented, but an increasing number of

researchers point out the negative effects of uncontrolled and unmitigated technological dissemination [1], [2]. In the absence of systemic and comprehensive proactive surveillance, accelerated technological abilities can create nuanced ethical and legal dilemmas. These gray areas regularly push the envelope of traditional legal boundaries, testing age-old moral paradigms.

Problems such as autonomous artificial intelligence, pervasive corporate surveillance, monetization of data, and weaponized misinformation illustrate why academic and regulatory intervention is urgently needed. Regulatory legal frameworks naturally lag behind growing software solution development, and this leads to the urgent need to establish robust ethical frameworks, develop comprehensive compliance with the platforms, and foster critical public awareness as the first priority. Finding the right balance between innovation, human dignity and structural safety is one of the key governance challenges of the modern digital era.

In emerging socio-economic realities and changing regional structures, the uneven path of digital access has served to entrench the structural disparities referred to as the digital divide [3]. The divide is seen through deficiencies in infrastructure, cost of acquiring technologies, and differing levels of digital literacy. Indeed, in more digitized public spaces, we have seen law enforcement and the judiciary gain more cutting-edge tools thanks to technology: AI-enabled predictive analytics tools, real-time cryptographic verification, and advanced digital forensics. These tools enhance operational capability to fight organized cybercrime and ensure regulatory compliance with cybercrime control, yet also present vulnerabilities to complex manipulation.

The technology's exact same tech stacks are being used by malicious actors to forge data, hide cyber-evidence, and automate identity theft. The paradox of two-way deployment of this dual-use dilemma suggests one way that modern societies operate in a complex dialectic: state-of-the-art computing resources serve as tools both for increased security and instruments of unparalleled systemic subversion. Reaching this tension requires a deliberate reconciliation to regulatory systems, user privacy rights, and national security demands [4], [5].

In addition, the growing footprint of automation and enterprise machine learning models is also effectively re-engineering the worldwide labor market. This shift also brings us to critical structural challenges regarding economic displacement, demands for institutional retraining and job replacement, and the decline of classical forms of employment [6], [7]. Crucially, though, autonomous decision-making engines cannot be viewed as neutral/objective. Considering that these algorithms mirror the data pipelines that underlie their logic, any historical or structural bias and structural anomalies are magnified and entrenched. This

makes continuous human-in-the-loop validation an absolute necessity. As large language models (LLMs) and conversational generative agents, such as OpenAI's ChatGPT, rapidly democratize, this also affects academic and corporate paradigms. As a result, disputes over intellectual property rights, the ethics of authorship, and data scraping for one's own interests also become very intense, for example, in court. Outside the workplace, the widespread integration of behavioral optimization algorithms into mainstream social media platforms has been directly linked with a variety of psychological stresses, from severe social anxiety or intense despair symptoms in various fields, to compulsive design-induced addiction. In such a growing ecosystem of technology, contemporary society should develop comprehensive frameworks that encourage engineering innovation alongside strict ethical responsibility.

Such sociotechnical volatility is amplified by the structural threat from algorithmic misinformation and coordinated fake news campaigns, and through them, the disruption of public discourse and the trade-offs between free speech and platform moderation. The deployment of AI-supported content recommendation loops speeds this diffusion, allowing for the propagation of disinformation through digital networks on an unprecedented scale and at blistering speed. At the same time, deepfake synthetic media represents a significant threat to digital trust, offering easily accessible avenues for political sabotage, corporate deception, and targeted damage to reputation [8], [9]. And with a democratization of access to generative media toolsets, platform builders and creators have an obvious moral and professional responsibility to ensure cryptographic verification and provenance tracing. Tech conglomerates need to turn away from profit-oriented algorithmic maximization, and toward models that are designed more toward promoting cognitive health and structural information integrity of the user [10], [11]. To support this transition, we need a mix of automated AI content moderation, transparent platform curation metrics, and stringent sovereign regulatory frameworks.

Though these technological risks are acknowledged globally in the abstract, a crucial research question persists: Are certain regional societies adequately mindful of and ready for these risks? This question is especially relevant in burgeoning countries as culturally cohesive countries such as the United Arab Emirates (U.A.E.). This study aims to establish the empirical baseline of awareness toward these disruptive

vectors in young Emirati citizens with theoretical technical training in Computer Information Sciences. The research tests the socio-technical resilience of a critical future leadership cadre as it maps the perspectives of this demographic on the long run.

## 2 Research Methodology and Objectives

The empirical aim of the study is to assess and characterize the structural awareness profile of top-tier Emirati computing students for the layered effects on their social, cultural, and professional environment in the current era of technologies. To systematically realize this higher-level objective, the research sets out the following operational research objectives:

- To assess the critical reaction to fast adoption of information technology on its ability to reshape norms, basic ethical beliefs, and traditional religious values, while measuring student concern regarding future structural disruptions.
- To assess participant knowledge regarding the progressive digital divide and its broader socio-economic effects on underprivileged or technically under-represented groups in society.
- To investigate student understanding of the expanded exploit surfaces and ethical vulnerabilities enabling financial misconduct, corporate fraud, and automated cybercrime.
- To determine the extent to which participants comprehend the psychological risks associated with chronic digital interaction, targeting algorithmically induced technostress, isolation, and dopamine-dependent platform reliance.
- To assess an understanding of the effects of weaponized misinformation and false information on public cognition, as well as the practical and ethical challenges arising from achieving effective balance between free speech and content regulation.
- To determine the degree of awareness of the ethical and security challenges that synthetic media and deepfakes bring to the verification of digital assets and the trust of institutions.

From the particular discipline perspective, this research provides insights into adoption theories and models for technology applications, and subsequently information diffusion and sociotechnical governance models. This study presents us with actionable empirical evidence that identifies what it takes to design culturally relevant,

ethically sustainable IT architectures through an analysis of cognitive responses towards a select group of individuals, namely students. In addition, the findings clarify the kinds of digital competencies and ethical literacies required in order to manage complex cybersecurity threats, data privacy mandates, and automated machine learning biases. After all, this work can, in the end, lay the infrastructure of progressive public policies and educational policies of institutions that put equitable digital access at the forefront, provide technical responsibility in their education, and have a strong socio-technical governance process.

## 3 Literature Review and Theoretical Foundations

To develop a substantial analysis of the social impacts of emerging technologies, it is necessary to critically appraise the existing academic literature. This section maps out the current literature in four main parts: socio-cultural and religious adaptation; the changing mechanics of the digital divide; the evolution of cyber-physical exploits; and the psychological effect of long-term technological connectivity.

### 3.1 Socio-cultural Transformations and Religious Adaptation

The embeddedness of computing architectures in daily life has progressed from being purely a functional utility to becoming a significant contribution to contemporary identity construction and cultural change [12]. As interactive systems are embedded into the course of life, their operational qualities change the norms of actions, ethical base values, and spiritual practices. The importance of cultural adaptations into digital systems is the theme of scholars who stress the relationship between the design practices on an engineering level and usability indicators related to the cultural identity of users. For example, empirical data showed that those created during the generation of mobile platforms and social applications that were designed to directly reflect the cultural values found in the native language had higher user engagement and long-term retention [13]. Such architectural concord is more and more important in modern interface generation, where international platforms use local values to adhere to regional norms.

Concurrently, AI-driven recommendation systems deployed within social media platforms have been shown to influence user behavior by reinforcing existing preferences, creating filter

bubbles, and amplifying cultural or ideological biases [14]. Such algorithmic models facilitate highly targeted user engagement, creating personalized information environments that may contribute to cognitive polarization, shape public narratives, and influence moral beliefs [15]. That automatic influence is possible signifies the grave social and ethical obligations of platform designers and regulators. In addition, digital technologies have brought about unprecedented changes in religious practice, transforming how faith communities engage with traditional rituals and customs [16]. The widespread availability of religious applications, mobile scripture platforms, and synchronized prayer and ritual notification systems illustrates how longstanding religious practices have adapted to digital environments, enabling continuity through localized, time-sensitive services in an increasingly interconnected world.

### **3.2 The Development of the Digital Divide through Structure**

The digital divide constitutes a crucial structural challenge involving unequal access to hardware, unequal technical acumen, and asymmetrical potential to harness data resources for economic growth. This divide has emerged as a significant social risk, as it affects access to education, career mobility, health outcomes, and civic engagement in a digitally interconnected world economy. The research highlights the extent to which systemic crises, notably the COVID-19 pandemic, exacerbated and amplified structural disparities and highlighted significant inequities in network resilience, institutional access to hardware, and sophisticated technical literacy [17]. A number of individuals and groups who do not have reliable digital access encounter obstacles to essential educational resources, remote labour markets, and digital healthcare networks.

Significantly, current scholarship highlights that the digital divide (and by implication its related phenomena) has transitioned from the basic issue of obtaining physical devices to the operational literacy and efficacy of the use of that equipment [18]. This “second layer” of inequality restricts economic mobility and perpetuates social disparities that already exist. Moreover, the explosion of cutting-edge technical fields — like cloud architecture, automated machine learning, and enterprise data analytics — only exacerbates this divide as it requires distinct cognitive competencies that in-school institutions can fall short on equitably providing [19]. Addressing the systemic disparities involved in these economic imbalances will require

broader structural interventions through comprehensive infrastructure investment, affordable connectivity programming, and strong digital literacy programs at all levels. Cross-sector partnerships are critical if technology is to underpin large-scale social equity and not entrench old structural divides.

### **3.3 Cyber-physical Threats, Synthetic Media, and Data Governance**

The rapid migration of personal, commercial, and governmental enterprises to virtual environments has exponentially increased the global attack surface, revealing vulnerabilities in data governance and network security. The proliferation of web-facing services, although improving transactional efficiency, has run far ahead of fundamental user ethical training and corporate data governance protocols [20]. This misalignment leaves both the private sector and individuals exposed to complex cyber-physical threats, corporate espionage, and state-sponsored data breaches. Research has shown that modern information ecosystems are highly vulnerable to coordinated disinformation campaigns that exploit the architecture of social media platforms to disseminate false narratives, erode institutional trust, and undermine social cohesion [21].

This challenge is compounded by the advent of synthetic media platforms and deepfake generation technology that employ advanced generative adversarial networks (GANs) to produce highly realistic and deceptive audio and video outputs. And as scholars warn, deepfakes pose profound risks to political stability, corporate verification systems, and overall digital security [22]. Such an advance in deception could lead to high-fidelity identity theft by adversaries, manipulation of financial markets, and judicial intrusion through fabrications that defy traditional verification processes. Besides the above, automated algorithmic decision-making and automated mass surveillance are being rapidly implemented with little regulation for many issues, highlighting several important issues concerning systemic bias, data privacy violations, and unauthorized profiling [23]. These new threats must be tackled through a mix of high public media literacy rates, advanced cryptographic verification features, and a statutory data governance regime.

### **3.4 Algorithmic Psychopathology and Technostress**

The psychological effects of constant technological adoption are also emerging clinical and sociological

paradigms. Researchers have defined ‘technostress’ as a unique psychological process where excessive structural dependence on digital communication tools negatively affects mental health, breaks work-life balance, and interpersonal relationships [24]. This pathology is also becoming more common in work-life systems that require an ‘unending constant digital presence’, leading to cognitive overload, fragmented attention, and emotional exhaustion. This is particularly pronounced within the context of social media ecosystems, where mediated interactions create spheres that can make up sites of power to push the boundaries of traditional human connections [25]. Although such networks serve as facilitators of global communication, they are robustly associated with increased rates of clinical anxiety, major depression, and social isolation in a younger population [26]. Constant peer-comparison loops, online harassment vectors, and compulsive platform engagement all contribute to this vulnerability.

Importantly, however, these adverse consequences are not accidental, but are, instead, motivated by the intentional designs of cyber-communicative social media platforms, which offer variable rewards as a way to enhance user screen-time [27]. Research on dopamine-dependent design loops has shown that real-time notifications and social validation metrics elicit unique compulsive neural reactions and establish a mental dependency [28]. This observation is bolstered by empirical research of the relationship between high smartphone use metrics and significant cortisol levels, extreme sleep disturbance, and reduced emotional endurance [29]. Moreover, there has been an increasing normalization of remote working options, the use of digital monitoring technologies, and the blurring of the line between personal and professional environments, leading to burnout driven by the expectation of 24/7 service availability [30].

## 4 Empirical Methodology and Data Collection

To evaluate the structural awareness profiles of next-generation Emirati IT professionals, this study deployed a quantitative, survey-based empirical methodology. This approach allowed for the systematic collection, statistical validation, and thematic analysis of participant responses relative to the identified sociotechnical risk domains.

### 4.1 Sample Characteristics and Selection Strategy

Owing to strict operational constraints and the need to evaluate a highly specific technical demographic, a non-probability convenience sampling strategy was utilized. The target population comprised upper-level undergraduate students enrolled in the third and fourth years of the bachelor's program in Computer Information Sciences (CIS) at a premier federal higher education institution in the United Arab Emirates. A cohort of 280 advanced students was invited to participate; a total of 200 fully completed, verified survey instruments were recovered, representing a highly robust response rate of 71.4%. The participant demographic was strictly bounded between the ages of 18 and 25, representing the next generation of technology professionals. All participation was completely voluntary, and no material or financial inducements were provided.

### 4.2 Instrument Development and Construct Validation

The quantitative instrument was constructed across two primary conceptual axes: (a) participant awareness of the structural impacts of rapid IT growth on social norms, corporate ethics, and traditional behaviors; and (b) critical perceptions regarding the influence of social media platforms on cognitive health and informational integrity. Each primary axis contained three explicit sub-constructs aligned with the core research questions.

To ensure construct validity, the survey was reviewed by an expert panel of six senior faculty members specializing in Computer Information Sciences. Minor structural modifications were applied based on their evaluations to ensure linguistic clarity and technical precision. The complete research protocol—including the Participant Information Sheet, formal Consent Documentation, and the final Survey Instrument—received formal institutional approval from the Research Ethics and Integrity Committee (REIC).

To establish internal consistency and reliability, each of the six core constructs was measured using four internal items phrased in the same direction. Responses were captured using a 5-point Likert scale: 5 (Strongly Agree), 4 (Agree), 3 (Neutral), 2 (Disagree), and 1 (Strongly Disagree). To avoid forced responses on complex topics, a non-parametric option—0 (Don't Know / Can't Say)—was included. Item ordering was randomized across the deployment interface to mitigate response bias and ensure data reliability. The scale's reliability

was validated by calculating Cronbach's alpha coefficient for each construct, applying an explicit academic acceptance threshold of  $\alpha \geq 0.70$ .

### 4.3 Field Administration and Ethical Controls

The empirical survey was administered between November 15 and November 30, 2024, across eight separate class groups of a required third-year Computer Science course. The digital survey was deployed via Microsoft Forms, with an average completion time of 10 minutes. Strict ethical controls were applied throughout the process: participants were required to review a digital Information Sheet and execute a mandatory Consent Form before unlocking the survey. Complete anonymity was maintained; no personally identifiable information (PII), such as names, student identifiers, or contact details, was collected. Participants retained the right to withdraw at any stage without penalty, and all data was processed aggregately for statistical evaluation.

## 5 Empirical Findings and Data Analysis

The data analysis was structured to answer the six core research questions, organized into two thematic domains: the macro-societal impacts of rapid IT adoption in the U.A.E., and the downstream socio-psychological risks of persistent social media use. The following section details the statistical findings for each construct.

### 5.1 Macro-Societal Impacts of Information Technology in the U.A.E.

The first thematic domain investigated how advanced IT infrastructures reshape the broader socio-cultural, economic, and ethical realities of the United Arab Emirates.

#### Construct 1: Re-engineering of Societal Norms, Core Ethical Principles, and Religious Traditions.

This construct evaluated the long-term transformative impact of IT infrastructure on cultural baselines. The collected data demonstrated a strong consensus: 66.25% of the technical cohort agreed that rapid technological advancement would significantly alter cultural norms and traditional religious values (22.75% Strongly Agree; 43.50% Agree). A neutral position was held by 24.25%, while a minor 6.0% disagreed (3.38% Disagree; 2.63% Strongly Disagree). Only 3.50% selected the

non-parametric option. The construct achieved a mean score of 3.80 and a Cronbach's alpha of 0.74, validating its internal consistency (Fig. 1).

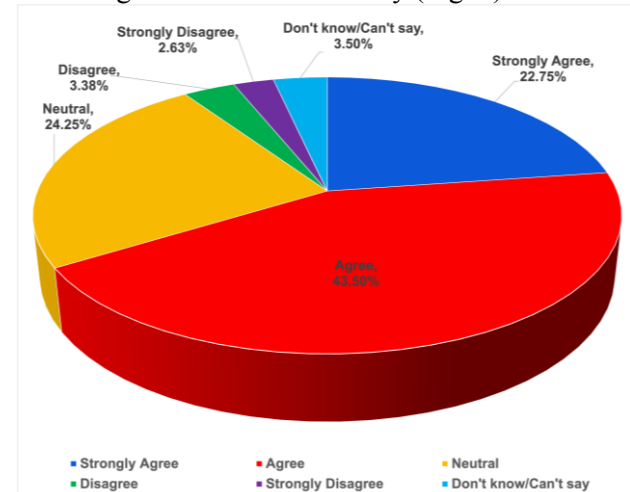


Fig. 1: Rapid IT progress will significantly reshape societal norms, ethical values, and religious beliefs  
Source: created by the authors

#### Construct 2: Intensification of the Digital Divide and Resource Disparities.

This construct measured awareness of technology-induced social stratification. The data showed that 66.25% of participants recognized that advanced IT distribution widens the digital divide, creating significant disparities based on resource availability (23.50% Strongly Agree; 42.75% Agree). A neutral stance was maintained by 27.50%, while only 2.75% expressed disagreement (2.25% Disagree; 0.50% Strongly Disagree). The remaining 3.50% reported unfamiliarity with the topic. The construct mean reached 3.78, with a robust Cronbach's alpha of 0.79, indicating strong reliability (Fig. 2).

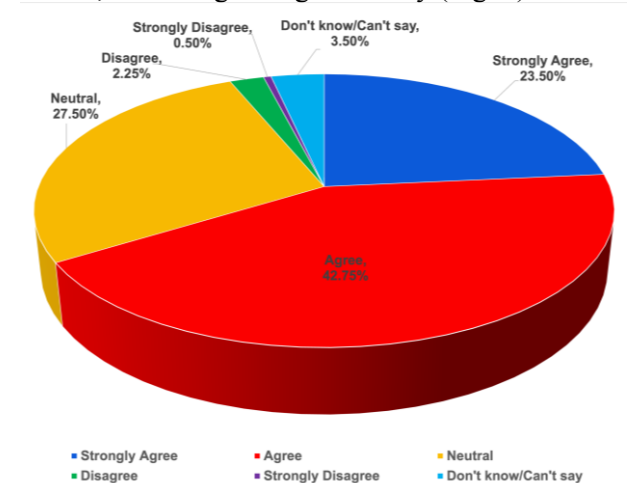


Fig. 2: IT developments significantly affect the digital divide, resulting in differences in access to technology depending on individuals' available technological resources  
Source: created by the authors

### Construct 3: Proliferation of Unethical and Exploitative Digital Vectors.

This construct assessed student comprehension of expanded cyberattack surfaces. The statistical results revealed that 64.88% of respondents agreed that rapid IT developments expand opportunities for corporate fraud, financial misconduct, and unethical behavior (24.50% Strongly Agree; 40.38% Agree). The neutral option was chosen by 24.88%, while 6.01% disagreed (4.63% Disagree; 1.38% Strongly Disagree); 4.25% were unable to respond. This construct returned a mean score of 3.74 and a high Cronbach's alpha of 0.85, confirming strong data reliability (Fig. 3).

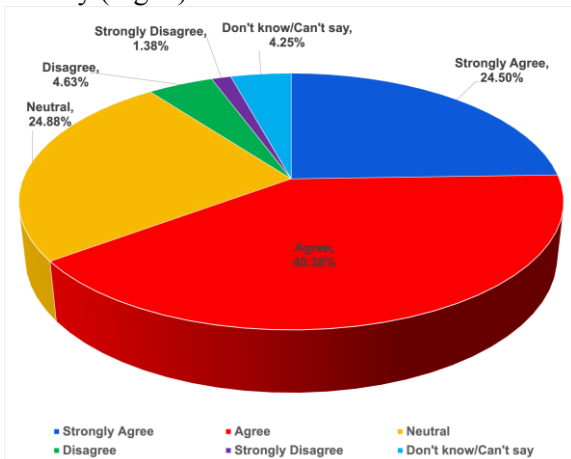


Fig. 3: Rapid IT developments increase the opportunities for businesses and individuals to engage in unethical and illegal behavior

Source: created by the authors

## 5.2 Downstream Psychological and Informational Risks of Social Media Platforms

The second domain focused on the psychological impacts of persistent connection and the security risks associated with synthetic media.

### Construct 4: Algorithmically Induced Psychopathology and Technostress.

This construct evaluated awareness of platform-induced mental health issues. The survey data indicated a high level of concern: 69.13% of the technical cohort agreed that constant connectivity and engagement-driven social algorithms directly contribute to clinical anxiety, depression, and social isolation (27.63% Strongly Agree; 41.50% Agree). A neutral position was held by 22.63%, whereas a minor 3.13% disagreed (2.50% Disagree; 0.63% Strongly Disagree); 5.13% selected the non-parametric option. The construct mean was 3.80, with a high Cronbach's alpha of 0.85, indicating strong internal validity (Fig. 4).

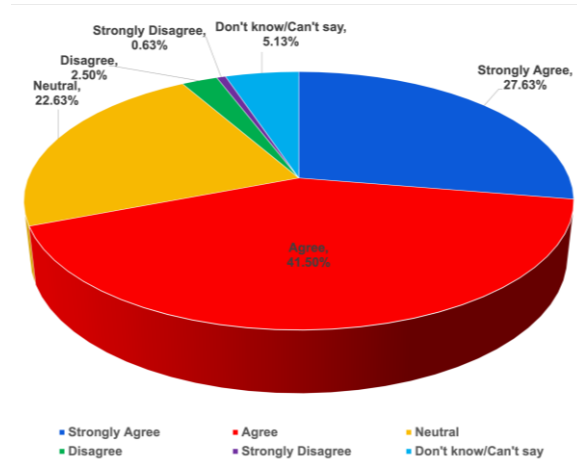


Fig. 4: There is a strong positive correlation between constant internet connectivity and social media manipulation of human behavior, which contributes to the occurrence of mental health issues like anxiety, depression, isolation, and addiction  
Source: created by the authors

### Construct 5: Weaponized Misinformation, Fake News, and Platform Governance Dilemmas.

This construct focused on the impact of false information on social stability. The data revealed that 70.50% of respondents recognized that fake news significantly alters public perception and agreed that balancing free expression with strict content regulation is an essential requirement for modern communication (31.25% Strongly Agree; 39.25% Agree). A neutral stance was maintained by 21.13%, while 4.25% expressed disagreement (3.50% Disagree; 0.75% Strongly Disagree). The remaining 4.13% reported unfamiliarity with the topic. The construct returned a high mean score of 3.87 and a Cronbach's alpha of 0.84 (Fig. 5).

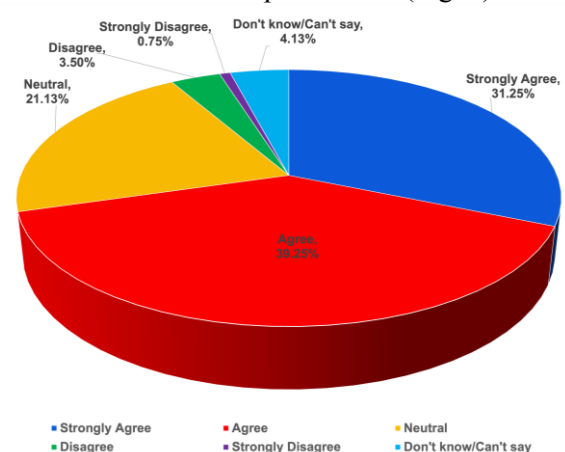


Fig. 5: Misinformation and fake news on social media significantly impact societal behavior, and balancing free speech with the regulation of false information is necessary for effective communication  
Source: created by the authors

### Construct 6: Proliferation of Deepfakes, Synthetic Media, and Erosion of Digital Trust.

This final construct measured participant awareness of the security and verification challenges introduced by AI-generated content. The empirical analysis showed that 70.13% of the technical students agreed that high-fidelity deepfakes seriously compromise the credibility of digital communication and create major ethical validation challenges (31.75% Strongly Agree; 38.38% Agree). A neutral position was held by 23.75%, while a negligible 2.26% disagreed (1.63% Disagree; 0.63% Strongly Disagree); 4.25% were unable to analyze the topic. The construct achieved a mean of 3.80 and a Cronbach's alpha coefficient of 0.85, establishing strong internal reliability (Fig. 6).

From an educational and policy perspective, these empirical results provide two crucial insights. First, advanced Emirati technology students exhibit a highly sophisticated understanding of the societal, ethical, and macro-economic disruptions caused by rapid technological growth. Second, they demonstrate a clear, critical awareness of the systemic risks associated with social platforms, cognitive manipulation, and synthetic media. Given that this surveyed cohort is on track to occupy critical management and engineering positions within the national digital ecosystem, their advanced awareness profile indicates that future technology leaders are well-positioned to design and implement proactive sociotechnical governance frameworks.

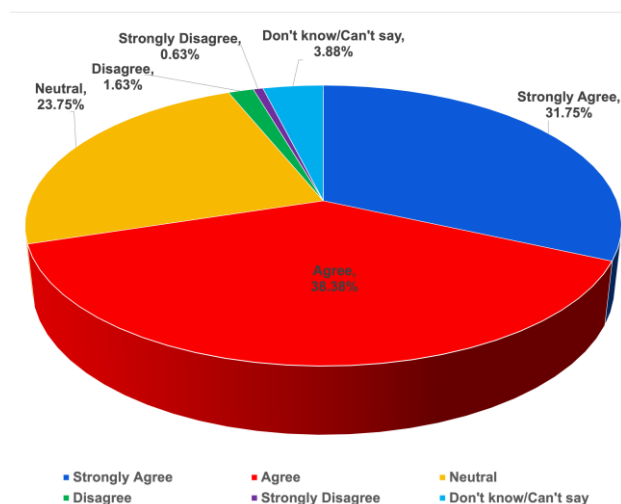


Fig. 6: Deepfakes – videos or audio recordings that appear real but are fabricated – significantly impact the trustworthiness of digital content, and they pose serious ethical concerns regarding the identification of fabricated media

Source: created by the authors

## 6 Conclusion and Next Steps

This article attempts to clarify the leading sociotechnical problems of the post-accelerated adoption of information technology and the efficient use of social media tools in the UAE through empirical work. The empirical relationships between continued digital connectivity, loop behavioral optimization, and psychological challenges such as clinical technostress, anxiety, and digital dependence have led us to examine the significance of holistic health programs and awareness campaigns. Because the overwhelming majority of the technical student respondents were concerned by these findings, the academic community and architects of public policy should work together in order to develop a new media literacy curriculum and guidance for what constitutes optimal digital activities.

As well, there is broad agreement around algorithmic misinformation and generative deepfakes, which indicates the need for robust regulatory instruments, automated verification systems, and well-defined legal lines so that information integrity in a digital realm does not deteriorate. Young Emirati computing professionals, especially, have developed a high degree of awareness at this level, which means that they are prepared to respond to complex policy developments and to monitor sophisticated technical security measures. These students will be integral members of the corporate, governmental, and engineering sectors, and critical thought, on the one hand, is a must for maintaining technological progress and promoting sustainability along with systemic responsibility. Ultimately, our project highlights the urgent importance of systemic education and strong, accountable governance to promote a resilient, secure, and ethical digital society in the UAE.

### Declaration of Generative AI and AI-assisted Technologies in the Writing Process

The authors wrote, reviewed and edited the content as needed and they have not utilised artificial intelligence (AI) tools. The authors take full responsibility for the content of the publication.

### References:

- [1] J. Danaher, "How technology alters morality and why it matters [Ethics]," *IEEE Robot. Autom. Mag.*, vol. 31, no. 2, pp. 147–148, 2024, doi: 10.1109/MRA.2024.3388278.
- [2] O. D. Nelson, "The effects of social media use on attitude changes of religious tolerance and intolerance: online social paradigms may bring new possibilities for transformations in

- organizations and society,” in *2022 IEEE Technology and Engineering Management Conference (TEMSCON EUROPE)*, IEEE, 2022, pp. 261–266. doi: 10.1109/TEMSCONEUROPE54743.2022.9801978.
- [3] P. Vassilakopoulou and E. Hustad, “Bridging digital divides: A literature review and research agenda for information systems research,” *Information systems frontiers*, vol. 25, no. 3, pp. 955–969, 2023, <https://doi.org/10.1007/s10796-020-10096-3>.
- [4] M. J. Quinn, “Ethics for the Information Age 8th edition,” *Print ISBN-13: 978-0135217726*, 2020.
- [5] G. Reynolds, *Ethics in information technology*, 6th Edi. Boston, MA: Cengage Learning, Print ISBN: 9781337405874, 2019.
- [6] M. Kaur, J. Kaur, and R. K. Kaur, “Adapting to technological disruption: challenges and opportunities for employment,” in *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, IEEE, 2023, pp. 347–352. doi: 10.1109/ICCCIS60361.2023.10425266.
- [7] G. Manoharan, P. Sharma, V. Chaudhary, P. C. Biswas, M. K. Sharma, and M. Lourens, “The future of work: examining the impact of AI/ML on job roles, organizational structures, and talent management practices,” in *2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies*, IEEE, 2024, pp. 1–6. doi: 10.1109/TQCEBT59414.2024.10545125.
- [8] D. Chapagain, N. Kshetri, and B. Aryal, “Deepfake disasters: A comprehensive review of technology, ethical concerns, countermeasures, and societal implications,” in *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, IEEE, 2024, pp. 1–9. doi: 10.1109/ETNCC63262.2024.10767452.
- [9] M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, “Deepfake detection: A systematic literature review,” *IEEE access*, vol. 10, pp. 25494–25513, 2022, doi: 10.1109/ACCESS.2022.3154404.
- [10] S. Lund et al., “The future of work in America: People and places, today and tomorrow,” *APO Australian Policy Online, McKinsey & Company*, 2019, [Online]. [https://apo.org.au/node/248901?\\_cf\\_chl\\_f\\_t\\_k=2147ltJMABiXqeS3aV50NpSRVyWe7\\_vUQCCdqRr5Hk-1782820470-1.0.1.1-gYvDHsdNIWY0Myzi5jPeR\\_fk2cQvsDsIxH\\_04GZJWLo#:~:text=RESOURCES,-The%20future%20of%20work%20in%20America%3A%20people%20and%20places%2C%20today%20and%20tomorrow,-DESCRIPTION](https://apo.org.au/node/248901?_cf_chl_f_t_k=2147ltJMABiXqeS3aV50NpSRVyWe7_vUQCCdqRr5Hk-1782820470-1.0.1.1-gYvDHsdNIWY0Myzi5jPeR_fk2cQvsDsIxH_04GZJWLo#:~:text=RESOURCES,-The%20future%20of%20work%20in%20America%3A%20people%20and%20places%2C%20today%20and%20tomorrow,-DESCRIPTION) (Accessed Date: January 10, 2026).
- [11] B. Aragona, *Algorithm audit: Why, what, and how?* Routledge, 1st Edition, 2021. doi: 10.4324/9781003080381.
- [12] P. Brey, “Ethical aspects of information security and privacy,” *Security, privacy, and trust in modern data management*, pp. 21–36, 2007, [https://doi.org/10.1007/978-3-540-69861-6\\_3](https://doi.org/10.1007/978-3-540-69861-6_3).
- [13] H. Hoehle, X. Zhang, and V. Venkatesh, “An espoused cultural perspective to understand continued intention to use mobile applications: a four-country study of mobile social media application usability,” *European journal of information systems*, vol. 24, no. 3, pp. 337–359, 2015, <https://doi.org/10.1057/ejis.2014.43>.
- [14] S. Milano, M. Taddeo, and L. Floridi, “Recommender systems and their ethical challenges,” *AI Soc.*, vol. 35, no. 4, pp. 957–967, 2020, doi: 10.1007/s00146-020-00950-y.
- [15] M. Cinelli, G. De Francisci Morales, A. Galeazzi, W. Quattrociocchi, and M. Starnini, “The echo chamber effect on social media,” *Proceedings of the National Academy of Sciences*, vol. 118, no. 9, p. e2023301118, Mar. 2021, doi: 10.1073/pnas.2023301118.
- [16] H. A. Campbell and R. Tsuria, *Digital religion: Understanding religious practice in digital media*. Routledge, 2021. doi: 10.4324/9780429295683.
- [17] S. Lythreath, S. K. Singh, and A.-N. El-Kassar, “The digital divide: A review and future research agenda,” *Technol. Forecast. Soc. Change*, vol. 175, p. 121359, 2022, doi: 10.1016/j.techfore.2021.121359.
- [18] A. J. A. M. Van Deursen and J. A. G. M. Van Dijk, “The first-level digital divide shifts from inequalities in physical access to inequalities in material access,” *New Media Soc.*, vol. 21, no. 2, pp. 354–375, 2019, <https://doi.org/10.1177/1461444818797082>.
- [19] S. Nambisan, M. Wright, and M. Feldman, “The digital transformation of innovation and entrepreneurship: Progress, challenges

- and key themes,” *Res. Policy*, vol. 48, no. 8, p. 103773, 2019, <https://doi.org/10.1016/j.respol.2019.03.018>.
- [20] J. Petrie-Wyman, A. Rodi, and R. McConnell, “Why should I behave? Addressing unethical cyber behavior through education,” *Developments in Business Simulation and Experiential Learning*, vol. 48, 2021, [Online]. <https://absel-ojs-ttu.tdl.org/absel/article/view/3309> (Accessed Date: January 15, 2026).
- [21] S. Vosoughi, D. Roy, and S. Aral, “The spread of true and false news online,” *Science* (1979), vol. 359, no. 6380, pp. 1146–1151, Mar. 2018, doi: 10.1126/science.aap9559.
- [22] C. Vaccari and A. Chadwick, “Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news,” *Soc. Media Soc.*, vol. 6, no. 1, p. 2056305120903408, 2020, <https://doi.org/10.1177/2056305120903408>.
- [23] A. Arunagiri and A. Udayaadhithya, “Governing artificial intelligence in post-pandemic society,” in *Global Pandemic and Human Security: Technology and Development Perspective*, Springer, 2022, pp. 413–433. [https://doi.org/10.1007/978-981-16-5074-1\\_22](https://doi.org/10.1007/978-981-16-5074-1_22).
- [24] E. Rohwer, J.-C. Flöther, V. Harth, and S. Mache, “Overcoming the ‘dark side’ of technology—a scoping review on preventing and coping with work-related technostress,” *Int. J. Environ. Res. Public Health*, vol. 19, no. 6, p. 3625, 2022, <https://doi.org/10.3390/ijerph19063625>.
- [25] T. Dienlin and M. J. Metzger, “An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample,” *Journal of Computer-Mediated Communication*, vol. 21, no. 5, pp. 368–383, 2016, <https://doi.org/10.1111/jcc4.12163>.
- [26] F. Lai, L. Wang, J. Zhang, S. Shan, J. Chen, and L. Tian, “Relationship between social media use and social anxiety in college students: Mediation effect of communication capacity,” *Int. J. Environ. Res. Public Health*, vol. 20, no. 4, p. 3657, 2023, <https://doi.org/10.3390/ijerph20043657>.
- [27] CEO TODAY, “How Social Media Algorithms Control Our Mental Well-Being,” CEO TODAY, [Online]. <https://www.ceotodaymagazine.com/2024/12/how-social-media-algorithms-control-our-mental-well-being/> (Accessed Date: January 15, 2026).
- [28] H. B. Macit, G. Macit, and O. Güngör, “A research on social media addiction and dopamine driven feedback,” *Journal of Mehmet Akif Ersoy University Economics and Administrative Sciences Faculty*, vol. 5, no. 3, pp. 882–897, 2018, <https://doi.org/10.30798/makuiibf.435845>.
- [29] J. D. Elhai, J. C. Levine, R. D. Dvorak, and B. J. Hall, “Fear of missing out, need for touch, anxiety and depression are related to problematic smartphone use,” *Comput. Human Behav.*, vol. 63, pp. 509–516, 2016, <http://dx.doi.org/10.1016/j.chb.2016.05.079>.
- [30] K.-L. Tan and P. F. Yeap, “The impact of work engagement and meaningful work to alleviate job burnout among social workers in New Zealand,” *Management Decision*, vol. 60, no. 11, pp. 3042–3065, 2022, <https://doi.org/10.1108/MD-05-2021-0689>.

#### Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Dimitrios Xanthidis and Ourania K Xanthidou: Supervised all the processes related to the research, contributed to the survey creation and administration, prepared the data analysis and findings section.
- Moataz Salhab, Anang Hudaya Muhamad Amin, Abdelrahman Abdelgader and Alya Alhammadi: Assisted in the creation and administration of the survey, in the data collection process, and, in part, in the writing of the various findings sections.
- Alya Yousef Abdulla Alhammadi: Assisted with the admin of the survey and the data collection process.

#### Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

#### Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

#### Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

[https://creativecommons.org/licenses/by/4.0/deed.en\\_US](https://creativecommons.org/licenses/by/4.0/deed.en_US)

