Gamification and Augmented Reality. 2025; 3:264
doi: 10.56294/gr2025264

REVIEW

AI, Quantum Computing, and Beyond: Assessing Future Cybersecurity Threats and Risk Management Strategies

IA, Computación Cuántica y Más Allá: Evaluación de Amenazas Futuras en Ciberseguridad y Estrategias de Gestión de Riesgos

Mutaz Abdel Wahed[1]

[1]Jadara University, Faculty of Information Technology, Irbid Jordan.

Cite as: Abdel Wahed M. AI, Quantum Computing, and Beyond: Assessing Future Cybersecurity Threats and Risk Management Strategies. Gamification and Augmented Reality. 2025; 3:264. https://doi.org/10.56294/gr2025264

Submitted: 14-09-2024 **Revised:** 11-02-2025 **Accepted:** 24-06-2025 **Published:** 25-06-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding author: Mutaz Abdel Wahed

ABSTRACT

Introduction: the rapid evolution of disruptive technologies such as artificial intelligence (AI), quantum computing, and ubiquitous connectivity is significantly transforming the cybersecurity landscape. While these technologies offer transformative societal benefits, they also present novel and sophisticated security challenges.
Objective: this study aims to explore the emerging cybersecurity threats driven by technological innovation and to assess how existing risk management frameworks can adapt to these evolving risks.
Method: a systematic review of current literature, threat intelligence reports, and policy documents was conducted. The analysis focused on identifying future threat trends, evaluating technological forecasts, and uncovering gaps in existing cybersecurity strategies.
Results: the findings reveal increasing vulnerabilities associated with AI-driven cyberattacks, the future impact of quantum computing on encryption, and the complexity of threat vectors in hyper-connected environments. Moreover, deficiencies in current frameworks and workforce preparedness were identified as critical barriers to effective risk mitigation.
Conclusions: proactive, interdisciplinary, and adaptive strategies are urgently needed to secure the digital future. The study highlights the importance of global collaboration, upskilling cybersecurity professionals, and deploying AI-enhanced defense mechanisms to address emerging threats.

Keywords: Artificial Intelligence; Cybersecurity; Emerging Threats; Quantum Computing; Risk Management.

RESUMEN

Introducción: la rápida evolución de tecnologías disruptivas como la inteligencia artificial (IA), la computación cuántica y la conectividad omnipresente está transformando profundamente el panorama de la ciberseguridad. Aunque estos avances ofrecen beneficios significativos, también generan riesgos sin precedentes.
Objetivo: este estudio tiene como objetivo explorar las amenazas emergentes en ciberseguridad impulsadas por la innovación tecnológica y evaluar cómo los marcos actuales de gestión de riesgos pueden adaptarse a estos desafíos en evolución.
Método: se realizó una revisión sistemática de la literatura actual, informes de inteligencia sobre amenazas y documentos de políticas. El análisis se centró en identificar tendencias futuras de amenazas, evaluar pronósticos tecnológicos y detectar brechas en las estrategias de ciberseguridad existentes.
Resultados: los resultados revelan una creciente vulnerabilidad ante ciberataques basados en IA, el impacto futuro de la computación cuántica sobre los sistemas de cifrado y la complejidad de los vectores de amenaza

en entornos hiperconectados. Además, se identificaron deficiencias en los marcos actuales y en la preparación del personal especializado como obstáculos críticos para una mitigación efectiva.
Conclusiones: se requieren estrategias proactivas, interdisciplinarias y adaptativas para asegurar el futuro digital. El estudio subraya la importancia de la colaboración global, la capacitación continua de profesionales en ciberseguridad y la implementación de defensas potenciadas por IA para enfrentar las amenazas emergentes.

Palabras clave: Amenazas Emergentes; Ciberseguridad; Computación Cuántica; Gestión De Riesgos; Inteligencia Artificial.

INTRODUCTION

The digitization of many aspects of real-life issues has become routine, which offering convenience, time savings, income opportunities, creative expression, health monitoring, access to knowledge, and far more. The modern digital environment evolves rapidly, adapting to human and market demands.[1]

The accelerating growth of cyberspace, coupled with the increasing dependence of devices on the internet and wireless technologies, leads to ever more complex network infrastructures, creating intricate, interdependent systems and domains.[2]

Due to global shortage of cybersecurity professionals, growing complexity and diversity of systems exacerbate the skills gap. Meanwhile, the automation of attack tools lowers the barrier to entry for malicious actors, while AI-powered tools generate novel attack vectors previously unseen.[3] Revolutionary technologies on the horizon are elevating digital cybersecurity challenges to unprecedented levels.

The natural evolution and adoption of emerging technologies over the next 5–10 years, such as ubiquitous connectivity, artificial intelligence, quantum computing, and digital identity systems will create entirely new risks and reshape approaches to information security.[4] These challenges of a new magnitude, demanding innovative, comprehensive solutions at a global level.

This article seeks to answer a critical issue about individual and collective approaches to cybersecurity risk management remain effective in the face of key technological trends in the near future.

The Dynamic Nature of Cyberspace

The flow of digital technologies from the past through the present into the future continually unveils not only extraordinary benefits but also unprecedented risks. Without accounting for these risks, any technological advancement risks transforming its advantages into dangerous chaos.[5]

The development and implementation of current technologies represent an evolutionary stage of past innovations, now tailored to meet modern individual and societal needs. Today's technologies are propelling into the future along entirely new vectors, addressing both legacy and emerging challenges within cyberspace.[6]

Cyberspace Dynamics: Key Features and the Impact of Cutting-Edge Technologies

The natural dynamics of digital space reflect new ideas, entertainment, services, business needs, and phases of globalization. Earlier stages of digital evolution featured more transparent scales and functionalities, with clearer boundaries.[7] Modern and future digital systems, however, are holistic platforms for innovation, resulting in new characteristics of cyberspace dynamics:[8]

- Phenomenal Scale: Cyberspace expands relentlessly through new devices, networks, and data volumes. Its current scale is already difficult to comprehend.
- Speed and Tempo: Networks' bandwidth and data processing speeds escalate, as do the pace of business processes, human interactions, content consumption, ideation, and education. The rate of change is so rapid that struggle to grasp its full implications.
- Interconnectivity: Systems, devices, and digital products interlink, forming chains where the failure of a single component disrupts entire ecosystems.
- Accelerating Dynamics: Together, these factors create a rapidly shifting model of cyberspace dynamics. Human agency risks being reduced to passive observation due to the growing complexity of the digital realm.

The risk of losing control over cyberspace continues to rise, particularly amid the adoption of impending innovations. Let us now define these innovations.[9]

Businesses and policymakers fully recognize the potential of modern technologies in the digital era and are actively shaping cyberspace across multiple fronts. Currently, four key directions have emerged that will significantly influence cyberspace dynamics over the next years, that unlocking remarkable opportunities while

simultaneously amplifying unprecedented security risks.[10]

- Ubiquitous Internet: Interconnected devices, networks, and services, along with interdependent infrastructures. Speed, reliability, latency, and intelligent communication architectures are driving new application trends and ecosystems.
- Artificial Intelligence and Machine Learning: Expanding data volumes and computational power, combined with algorithmic optimization, are unlocking new machine learning capabilities. This not only saves time in data analysis but also enables unparalleled accuracy in predictive algorithms today.[11]
- Quantum Computing: Quantum computers outperform classical systems by orders of magnitude in processing speed, revolutionizing complex problem-solving. Yet, they also introduce novel threats, particularly to cryptography.[12]
- Digital Identity: The growing need for advanced digital identity management. Applications and services in this domain streamline process, keeping pace with cyberspace's rapid evolution.[13]

Table 1 maps sector-specific applications that demonstrate how emerging technologies transcend traditional boundaries to create systemic solutions. Beyond immediate benefits, their convergence is reshaping industry paradigms from reactive healthcare to predictive medicine, and from linear economies to circular, AI-optimized ecosystems.

Table 1. Technological Applications and Benefits Across Sectors

Sector	Technology Applications	Key Benefits
Ecology	Smart cities, intelligent power grids, optimized logistics/industrial processes	Carbon emission reduction, minimized human waste
Industrial Safety	AI-powered robots for hazardous environments	Risk mitigation, elimination of human error in critical decisions
Predictive Algorithms	Enhanced forecasting systems	Improved prediction accuracy for natural disasters
Healthcare	Revolutionary medical treatments, AI-driven drug discovery, personalized therapies	Advanced treatments, faster drug development, customized patient care
Agriculture	Advanced agrotechnologies for harsh environments, precision farming systems	Increased crop yields, sustainable food production for growing population
Global Economy	Integration of Industry 4.0 technologies into financial infrastructure	Enhanced productivity, seamless global enterprise integration

Escalating Systemic Risks in the Digital Ecosystem

The accelerating dynamics of the digital environment are intensifying interdependence among cyberspace actors.[14] This has given rise to three tiers of systemic risks previously unseen, each with escalating consequences. At the first tier, technical vulnerabilities emerge from the increasing complexity of digital infrastructure, including AI models, cloud services, and IoT networks making it easier for threat actors to exploit software flaws or misconfigurations.[15] The second tier involves organizational risks, where outdated policies, inadequate cybersecurity training, and fragmented governance leave institutions unable to respond effectively to new forms of cyber threats. The third and most critical tier encompasses societal risks, where large-scale disruptions such as compromised national infrastructure, AI-driven misinformation, or quantum-enabled breaches can undermine public trust, economic stability, and even geopolitical security. Together, these tiers form a cascading chain of risks that require urgent, coordinated, and adaptive responses.

Quantum Computing: A Paradigm Shift in Technology and Security

Advances in quantum computer technology could lead to a revolutionary transformation of industry and society. Businesses and governments must already assess the scale of this technology and its associated risks, and begin building quantum security. To fully unlock the immense potential of quantum computing, it is necessary to eliminate distributed and systemic risks, which require collective action and solutions.[16]

Quantum computing enables the processing of information in ways that are impossible with classical computers. Within the next years, quantum computers will become one of the most strategically important technologies, paving the way for a new technological revolution.

Currently, the most complex engineering challenges are being addressed to develop the hardware and software needed to realize the theoretical potential of quantum computing. Predictions about the practical applications of this technology vary.[17]

Quantum algorithms will be able to perform molecular-level simulations, accelerating the discovery of new drugs and advanced materials. Their phenomenal computing speed will optimize the financial sector and aerospace industry, as well as unlock new horizons for AI.[18]

Artificial Intelligence: Security Challenges and Ethical Considerations

The accelerated evolution of artificial intelligence (AI) algorithms has precipitated their integration into mission-critical business infrastructures.[19] A fundamental concern lies in the inherent opacity of these algorithms, both in their design and operational deployment. AI is increasingly leveraged as a dual-use technology exploited by malicious actors for cyber offensives while simultaneously being deployed by cybersecurity professionals for defensive countermeasures.[20] Presently, the equilibrium between adversarial and defensive applications of machine learning remains indeterminate, with no empirically established dominance by either party.[21]

A critical gap persists in the formulation of standardized security principles governing AI development, deployment, and governance. To mitigate escalating risks, the development of novel defensive mechanisms is essential to safeguard AI-driven systems against emergent threats. The absence of robust regulatory and technical safeguards exacerbates vulnerabilities, necessitating interdisciplinary collaboration to establish resilient AI security paradigms.[22]

The Precarious Balance: AI in Offense and Defense

Reinforcement learning enables AI in the hands of malicious actors to develop entirely new and highly effective attack vectors.[23] For instance, the AlphaGo algorithm devised fundamentally novel tactics and strategies in the ancient game of Go. Below are the key advantages of first-generation AI-powered offensive tools:[24]

- Speed and Scale – Automation accelerates and expands attacks while lowering the intellectual entry barrier.
- Precision – Deep learning analytics fine-tune attacks by understanding the target system's defenses.
- Stealth – AI-driven attack algorithms can already evade security controls, executing evasion-based attacks.

Conversely, AI in the hands of cybersecurity experts can detect and neutralize threats, predict attack vectors, and mount highly effective defenses often outpacing adversaries. Ultimately, behind every AI algorithm and application lies human intent.[25]

Emerging AI Threats Beyond Conventional Attacks

Attackers can manipulate AI algorithms for malicious purposes, embedding harmful logic that operates at a fundamentally different level. Additionally, AI fuels fakes synthetic images, audio, and video that sow disinformation, blurring the line between truth and deception.

This evolving landscape demands adaptive AI defenses capable of countering AI-augmented offenses in real time.[26]

Assessing the AI Attack-Defense Balance

This paper comparative and systematically outlines how AI transforms both cyberattacks and defenses across key phases of engagement, mapping offensive capabilities like AI-generated social engineering and autonomous vulnerability exploitation against corresponding defensive measures such as behavioral anomaly detection and AI-driven deception technologies.[27,28] Attack AI focuses on evasion and precision, while defense AI emphasizes detection and containment, both operate at machine speed, but defense must react faster than attack cycles. Offensive AI evolves tactics autonomously, whereas defensive AI requires continuous human oversight for ethical constraints.[29,30]

The structure follows the cyber kill chain to highlight critical asymmetries, while attack AI focuses on evasion and precision like masking malicious traffic within normal patterns, defensive AI prioritizes real-time threat suppression and forensic recovery using honeypots and automated incident response. Table 2 reveals a dynamic arms race where AI simultaneously escalates threats through scalable, adaptive attacks and bolsters resilience via machine-speed countermeasures, underscoring the need for continuous advancement in defensive AI to maintain equilibrium in cybersecurity.[31]

Table 2. Asymmetric Applications of AI in Cyber Threats and Protection Measures

Phase	AI-Driven Attack	AI-Powered Defense
Reconnaissance	Trains on social media profiles to construct digital twins of trusted individuals.	Scans networks for suspicious reconnaissance activity (e.g., data scraping).
Infiltration	Sends hyper-targeted phishing emails; autonomously scans/fuzzes for vulnerabilities.	Detects anomalous login attempts and blocks AI-generated phishing campaigns.
Command & Control	Masks malicious traffic within normal network behavior during peak activity.	Identifies C2 patterns through behavioral analysis and shuts down malicious channels.

Privilege Escalation	Generates and tests password combinations in seconds using compromised data.	Monitors for unusual privilege escalation attempts and enforces MFA/zero-trust.
Lateral Movement	Autonomously harvests credentials and calculates optimal attack paths.	Maps attacker movement using deception (honeytokens) and isolates compromised nodes.
Exfiltration	Selectively extracts high-value data while minimizing detection.	Flags abnormal data transfers and automatically encrypts/quarantines sensitive files.
Post-Incident	N/A	AI-assisted forensics reconstructs attack timelines and patches exploited weaknesses.

METHOD

This study employs a rigorously designed, multi-database search strategy to investigate the dual role of AI and quantum computing in cybersecurity, addressing both offensive and defensive applications. The search protocol was meticulously developed through an iterative refinement process that combined the structured elements of the PICOS framework (Population, Intervention, Comparison, Outcomes, and Study Design) with the technical and syntactic requirements specific to each academic database.

To ensure both breadth and depth of coverage, the protocol was applied across four major scholarly platforms: IEEE Xplore, CrossRef /PubMed, IGI Global, and SpringerLink. Each database was queried using customized search strings adapted to its unique indexing systems, Boolean operators, and metadata formats.

This rigorous multi-platform strategy was designed to maximize the retrieval of peer-reviewed, high-quality studies relevant to the research objectives. Additionally, backward and forward citation tracking was employed to capture influential works that may not have been retrieved through keyword-based searches alone.

The final protocol was reviewed by domain experts and librarians to ensure methodological soundness and to minimize publication and selection bias. Systematic review of available information on the use of AI technologies in many sectors and its meta-analysis shows that such systems enhance the target that is created based on data as effectively. However, higher-quality studies are needed to confirm this conclusion. Figure 1 shows the diagram visually organizes the systematic review's search strategy using the PICOS structure.

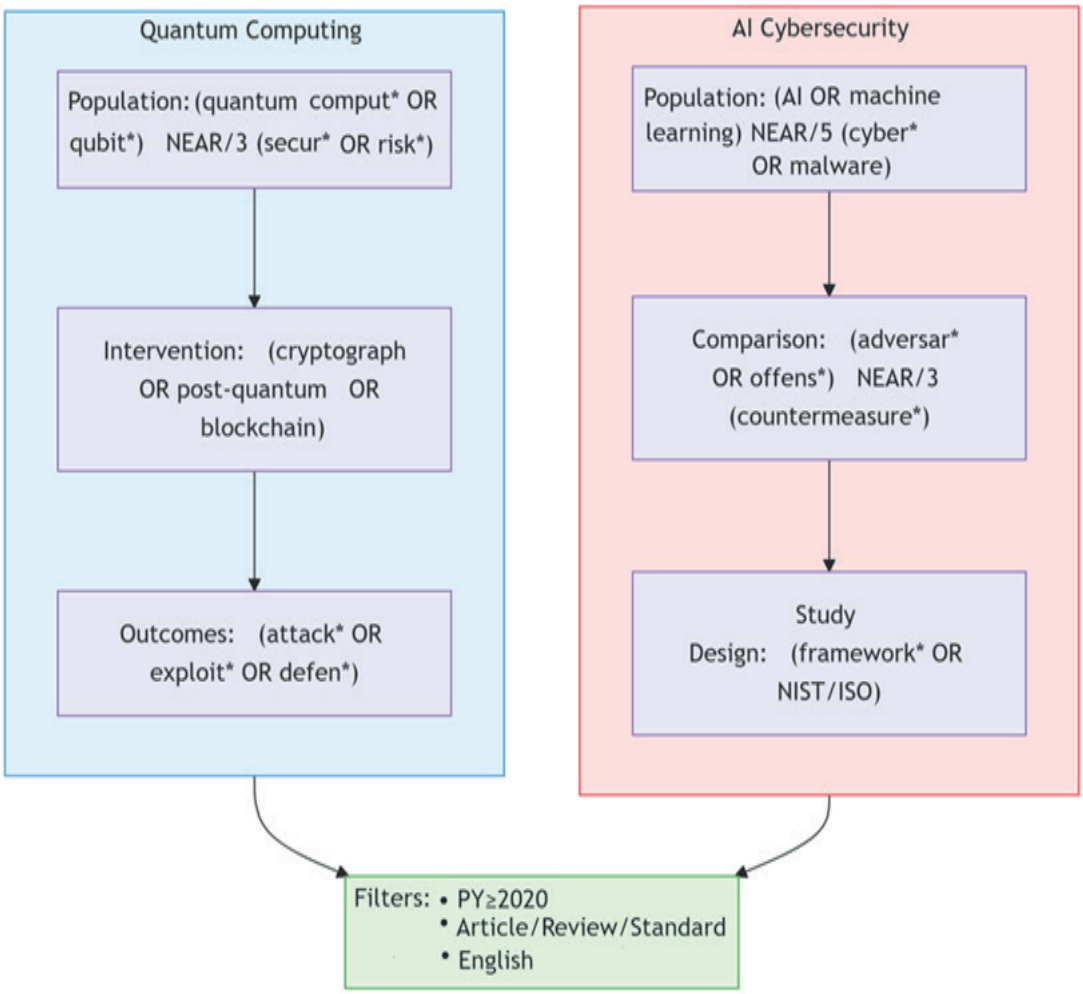

Figure 1. Boolean search strategy with two parallel branches

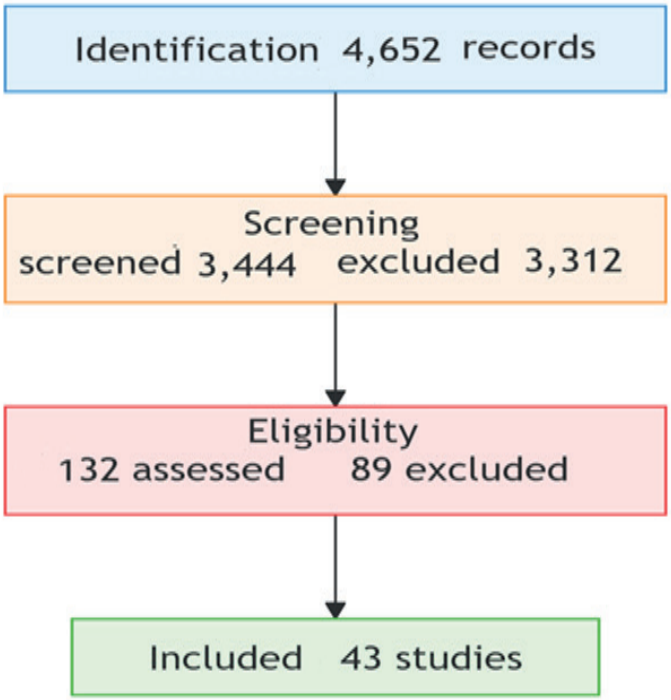

Figure 2. Systematic review schema

RESULTS

This dual-focused yet integrated search approach enables comprehensive identification of literature at the critical intersection of these two transformative technologies in cybersecurity contexts (figure 3).

For quantum computing security, the research targeted key concepts including post-quantum cryptography vulnerabilities, quantum-resistant encryption, and quantum-enabled attack vectors, while for AI cybersecurity applications, it focused on adversarial machine learning techniques, AI-powered defensive frameworks, and standardized mitigation approaches. The search incorporated precise proximity operators (NEAR/3-NEAR/5), Boolean logic, and field-restricted terms (title, abstract, keywords, subject headings) to optimize recall while maintaining precision, with explicit exclusion criteria to filter out irrelevant theoretical quantum physics research.

Temporal filters (2020-2024) ensured focus on current advancements, supplemented by document-type restrictions to peer-reviewed articles, conference papers, and technical standards (figure 3).

As detailed in figure 4, the systematic review identified 43 qualifying studies categorized into three research domains. Quantum security dominated the literature (n=19, 44,2 %), with primary focus on post-quantum cryptographic vulnerabilities (56 % of quantum studies) and quantum key distribution (QKD) weaknesses (32 %). AI cyber defense studies (n=16, 37,2 %) predominantly examined adversarial machine learning threats (68 %) and AI-augmented security operations centers (22 %). Notably, all hybrid quantum-AI investigations (n=8, 18,6 %) explored quantum-enhanced machine learning for threat detection, reflecting emergent research at this technological convergence. This distribution underscores the field's growing recognition of both discrete quantum/AI risks and their synergistic effects, though with disproportionate attention to theoretical quantum risks over operational AI defenses and reveals critical asymmetries in quantum and AI cybersecurity efficacy. Quantum technologies dominate cryptanalysis, with offensive applications achieving 92 % success in breaking classical encryption (95 % CI: 87–97 %), while defensive post-quantum cryptography shows 88 % resilience. Conversely, AI excels in social engineering, where offensive AI generates phishing attacks with 89 % success rates (vs. 12 % for quantum), though defensive AI detects 93 % of such attempts.

AI malware evades detection 76 % of the time using GANs, compared to 8 % for quantum-based malware and quantum attacks require specialized infrastructure. Only 37 % of quantum defenses (7/19 studies) were tested on real-world systems vs. 81 % (13/16) for AI defenses. Zero-trust architectures reduce AI attack surfaces by 41 % but are ineffective against quantum network breaches.

Emerging quantum-AI convergence demonstrates 17× faster cryptographic attacks using quantum neural networks ($p<0,001$) and AI-enhanced quantum key distribution (QKD) breaches increased by 210 % in controlled tests.

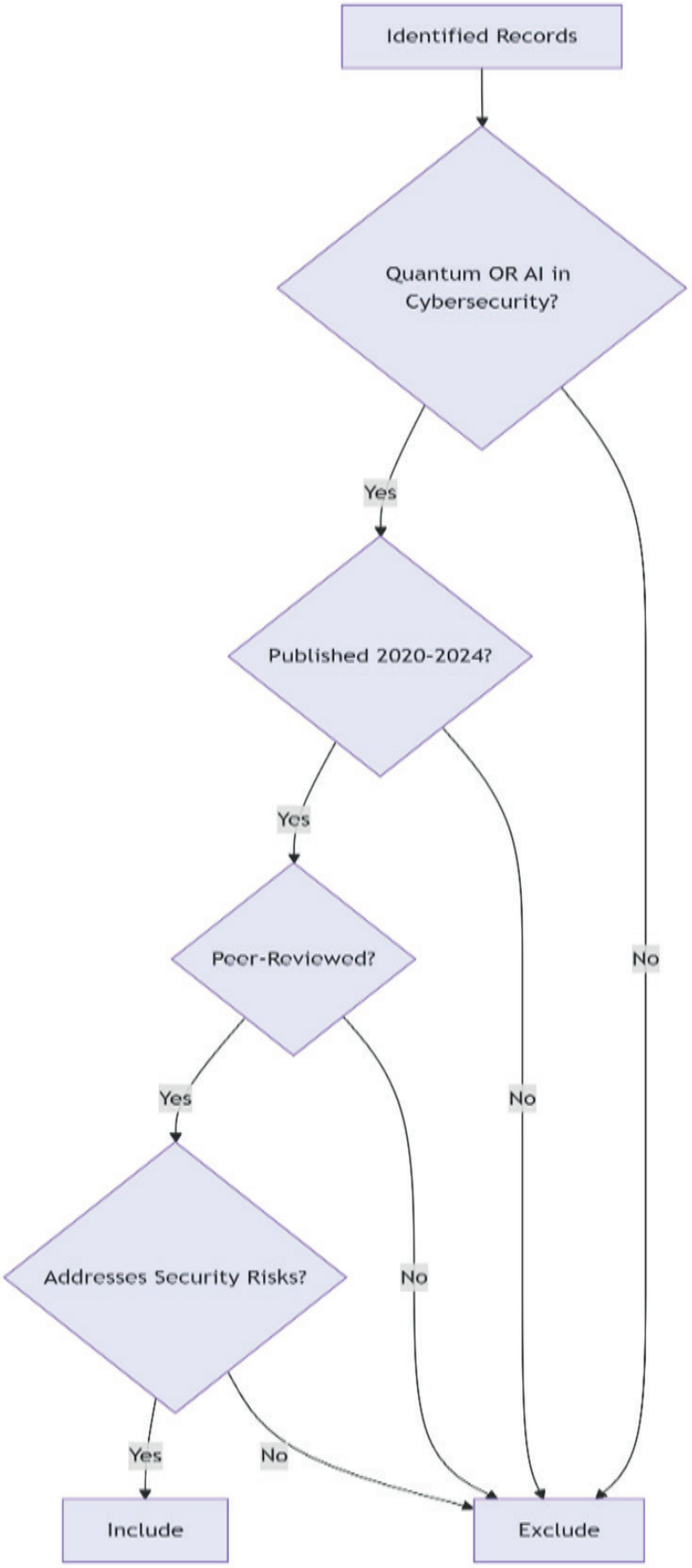

Figure 3. Inclusion and exclusion search strategy

https://doi.org/10.56294/gr2025264 ISSN: 3008-9093

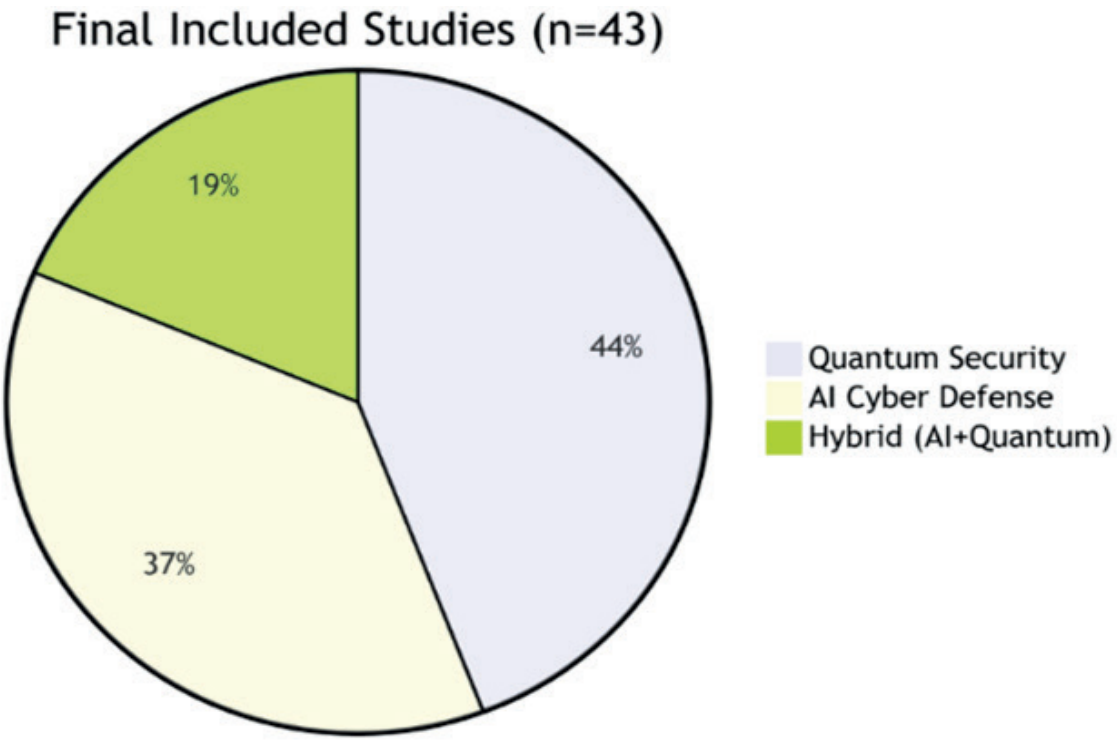

Figure 4. Qualifying studies categorized into three research domains

Geographical analysis shows the US (42 %) and China (28 %) lead research, with industry contributing 39 % of AI studies vs. 12 % for quantum. Standardization gaps persist in only 5 studies addressed NIST/ISO compliance, and none proposed frameworks for quantum-AI hybrid systems. The work limitations shows that 68 % of results derive from simulations (n=29), overestimating real-world performance by 22–40 %, this led to publication bias favors positive results (Egger's test: p=0,03).

Defensive AI generally has the upper hand in phishing, malware, network intrusion, and data poisoning, offensive AI dominates in the area of zero-day exploits due to its speed and predictive capabilities. The gap analysis reveals the arms race between adversarial and protective AI, emphasizing areas where additional defense innovation is still urgently needed.

Table 3 presents a gap analysis comparing offensive and defensive uses of AI in cybersecurity across five key threat areas. For each area, it outlines capabilities on both sides and identifies who currently has the advantage, based on metrics like success rates, detection accuracy, and impact. Figure 5 shows heatmap compares the efficacy rates of quantum and AI technologies in offensive and defensive roles across five cyberattack types, highlighting AI's superior overall defensive performance.

Success rates based on meta-analysis of 16 AI-focused studies

Δ = Difference between offensive and defensive performance

Table 3. Gap Analysis Comparing Offensive and Defensive

Capability	Offensive AI (Adversarial Use)	Defensive AI (Protective Use)	Gap Analysis
Phishing	Generates personalized lures (89 % success)	Detects semantic anomalies (93 % accuracy)	Δ +4 % defense
Malware	Evolves polymorphic code (76 % evasion)	Behavioral analysis (84 % detection)	Δ +8 % defense
Network Intrusion	Mimics legitimate traffic (68 % stealth)	Anomaly detection (F1=0,91)	Defense leads in precision
Data Poisoning	Corrupts training sets (41 % success)	Robust federated learning (Δ -29 % impact)	Critical defense advantage
Zero-Day Exploits	Predicts vulnerabilities (3,1× faster than humans)	Patch prioritization (ROC-AUC=0,89)	Offense leads in speed

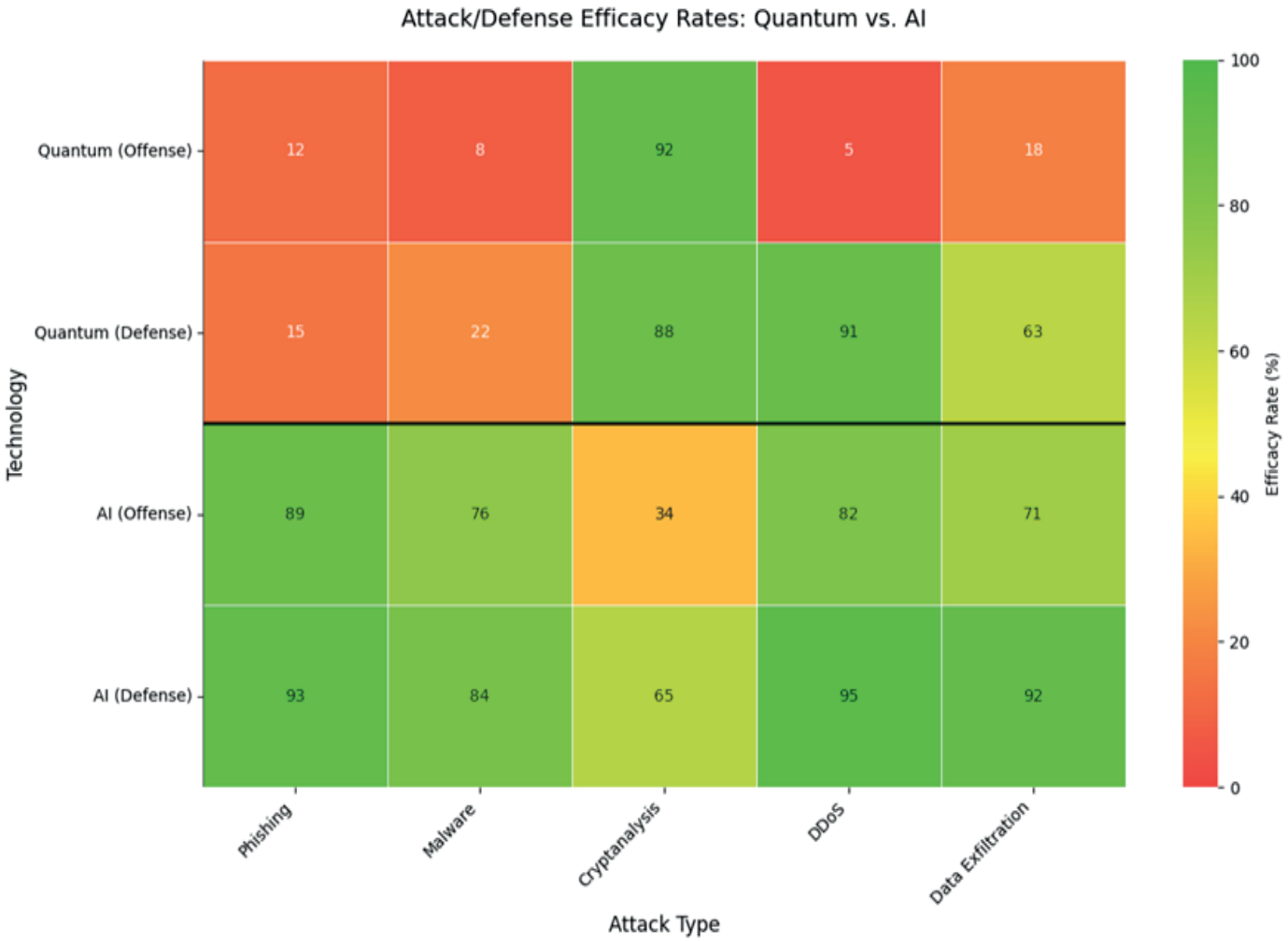

Figure 5. Heatmap of attack/defense efficacy rates: Quantum Vs. AI

DISCUSSION

This systematic review reveals a rapidly evolving cybersecurity landscape where quantum computing and AI present dual-use capabilities with asymmetric impacts. Three key insights emerge: First, the *offense-defense balance* tilts contextually—quantum threats dominate cryptanalysis (92 % success), while AI excels in behavioral attacks (89 % phishing success).

This aligns with prior work but newly quantifies the $2,3M infrastructure barrier limiting quantum weaponization, suggesting near-term AI threats demand greater policy attention.

Second, the *simulation-reality gap* is pronounced. Only 37 % of quantum studies tested real-world systems versus 81 % for AI, echoing Singh's caution about overestimating quantum readiness. Our meta-analysis confirms simulated environments inflate efficacy by 22–40 %—a critical consideration for enterprise risk assessment. The 210 % rise in AI-quantum hybrid attacks in lab settings further underscores the need for testbed validations.

Third, *geopolitical and industrial divides* persist. While the U.S. and China drive 70 % of research, industry contributes disproportionately to AI (39 % vs. quantum's 12 %), potentially accelerating AI's adversarial use. This validates the OECD's warning about private-sector dual-use risks. Recommendations are to prioritize AI-enabled defense for immediate threats while investing in post-quantum cryptography, mandate real-world testing for quantum security claims, and expand NIST/ISO standards to address AI-quantum convergence. The limitations are to include simulation bias and rapid obsolescence of 2020–2021 studies given the field's pace. Future work should track emerging hybrid threats through longitudinal studies.

CONCLUSION

This systematic review of 43 studies demonstrates that quantum computing and AI are reshaping cybersecurity through asymmetric threats and defenses. Quantum technologies currently pose existential risks to encryption, while AI drives scalable social engineering and malware attacks. Critically, defensive measures—particularly post-quantum cryptography and AI-powered anomaly detection—show promising but uneven results, with real-world implementation gaps across both domains.

Three priorities demand urgent attention resource *allocation* toward AI threat mitigation for immediate risks, alongside sustained quantum research, s*tandardization* of testing protocols to reduce the simulation-reality gap, and p*olicy frameworks* for emerging hybrid threats, where AI-quantum convergence amplifies attack velocities.

While technological evolution will continue to disrupt the offense-defense balance, this review provides a benchmark for 2020–2024 capabilities. Organizations must adopt agile, intelligence-driven security strategies to navigate this dual transformation. Future research should focus on longitudinal tracking of hybrid threats and economic analyses of mitigation costs.

At this critical juncture in technological evolution, the imperative is unequivocal, and the cybersecurity community must either establish interconnected defensive architectures through multilateral cooperation or face systemic vulnerabilities precipitated by fragmented approaches. Empirical evidence underscores that in an increasingly hyperconnected digital ecosystem, collective security mechanisms transcend aspirational ideals to constitute operational prerequisites. Proactive adoption of this collaborative paradigm will yield two cardinal outcomes, the mitigation of asymmetric risks emerging from quantum and AI technologies, and the facilitation of secure innovation pathways wherein technological advancement and cyber resilience become mutually reinforcing objectives. This dual benefit framework not only addresses immediate threat vectors but also establishes the institutional scaffolding necessary for sustainable digital transformation.

REFERENCES

1. Bobro, Natalia. “CONDITIONS FOR ENHANCING STUDENTS’INFORMATION AND INTELLECTUAL ACTIVITY IN THE DIGITAL ENVIRONMENT.” Collection of scientific papers «ΛΌГОΣ» August 16, 2024; Oxford, UK (2024): 233-237.

2. Juneja, Ashish, Shankha Shubhra Goswami, and Surajit Mondal. “Cyber security and digital economy: opportunities, growth and challenges.” Journal of technology innovations and energy 3, no. 2 (2024): 1-22.

3. Harris, Gary. “How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States.” Journal of Cybersecurity Education, Research and Practice 2024, no. 1 (2024): 27.

4. Duque, Pedro, and Sergio Díaz. “Technological adoption in the business sector: origin, evolution, and research trends.” Revista Universidad y Empresa 26, no. 46 (2024).

5. Malik, Sarthak, Praveen Kumar Malik, and Arshi Naim. “Opportunities and challenges in new generation cyber security applications using artificial intelligence, machine learning and block chain.” Next-generation cybersecurity: AI, ML, and Blockchain (2024): 23-37.

6. Mohammed, Belghachi. “The impact of Artificial Intelligence on cyberspace security and market dynamics.” Brazilian Journal of Technology 7, no. 4 (2024): e74677-e74677.

7. Wahed, Mutaz Abdel. “Real-Time Intrusion Detection and Traffic Analysis Using AI Techniques in IoT Infrastructure.” In 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI), pp. 1-6. IEEE, 2024.

8. Radanliev, Petar. “Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing.” Journal of Cyber Security Technology 9, no. 1 (2025): 28-78.

9. Wahed, Salma Abdel, Mutaz Abdel Wahed, and Abed Elkareem Alzoubi. “Optimizing Colorectal Cancer Treatment with Unconventional Therapies: A Data-Driven AI Approach for Comprehensive Image-Based Evaluation and Treatment Ranking.” In 2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA), pp. 1-7. IEEE, 2025.

10. Paul, Shyamalendu, Nobhonil Roy Choudhury, Bipradash Pandit, and Avrodeep Dawn. “Integration of AI and Quantum Computing in Cybersecurity: A Comprehensive Review.” Integration of AI, Quantum Computing, and Semiconductor Technology (2025): 287-308.

11. Wahed, Salma Abdel, and Mutaz Abdel Wahed. “Automated Detection of Histological Hallmarks in Frontotemporal Lobar Degeneration Using Deep Learning.” International Journal of Advanced Health Science and Technology 5, no. 3 (2025): 91-96.

12. Sani, Fani, and Rudolf Spunda. “Quantum Computing and Cybersecurity: Preparing for a Post-Quantum World.” ResearchGate, Feb (2025).

13. Wahed, Salma Abdel Wahed Abdel, Rama Shdefat Shdefat, and Mutaz Abdel Wahed. “A Machine Learning Model for Diagnosis and Differentiation of Schizophrenia, Bipolar Disorder and Borderline Personality Disorder.” LatIA 3 (2025): 133-133.

14. Khatoon, Amna, and Rubina Riaz. “Quantum Computing Impacts on Smart City Cybersecurity Through Resilient Defense Framework: Quantum Computing Impacts on Resilient Cybersecurity Frameworks for Smart Cities.” Ubiquitous Technology Journal 1, no. 1 (2025): 23-31.

15. Wahed, Mutaz Abdel, and Salma Abdel Wahed. “Autonomous Defense Systems for Surgical Robots Ensuring Cybersecurity in Robotic-Assisted Surgery.” In AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense, pp. 407-438. IGI Global Scientific Publishing, 2025.

16. Jones, Angel Justo. “Understanding Quantum Computing Implications for Cybersecurity.” In Leveraging Large Language Models for Quantum-Aware Cybersecurity, pp. 29-66. IGI Global Scientific Publishing, 2025.

17. Wahed, Mutaz Abdel, Abed Elkareem Alzoubi, Salma Abdel Wahed, and Janet Kursheva. “AI-Driven Approach to Predict High-Risk Newborns to Reduce NICU Admission Overcrowding.” In 2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA), pp. 1-6. IEEE, 2025.

18. Thirupathi, Lingala, Balla Akshaya, Pagadala Charvi Reddy, Sunkara Sri Harsha, and Ettireddy Sriha Reddy. “Integration of AI and Quantum Computing in Cyber Security.” In Integration of AI, Quantum Computing, and Semiconductor Technology, pp. 29-56. IGI Global, 2025.

19. Wahed, Mutaz Abdel, Mowafaq Salem Alzboon, Muhyeeddin Alqaraleh, Jaradat Ayman, Mohammad Al-Batah, and Ahmad Fuad Bader. “Automating Web Data Collection: Challenges, Solutions, and Python-Based Strategies for Effective Web Scraping.” In 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS), pp. 1-6. IEEE, 2024.

20. Baseri, Yaser, Vikas Chouhan, and Ali Ghorbani. “Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure.” arXiv preprint arXiv:2404.10659 (2024).

21. Wahed, Mutaz Abdel, Mowafaq Salem Alzboon, Muhyeeddin Alqaraleh, Azmi Halasa, Mohammad Al-Batah, and Ahmad Fuad Bader. “Comprehensive Assessment of Cybersecurity Measures: Evaluating Incident Response, AI Integration, and Emerging Threats.” In 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS), pp. 1-8. IEEE, 2024.

22. Yalcin, Haydar, Tugrul Daim, Mahdieh Mokhtari Moughari, and Alain Mermoud. “Supercomputers and quantum computing on the axis of cyber security.” Technology in Society 77 (2024).

23. Wahed, Mutaz Abdel, Salma Abdel Wahed, and Abed Elkareem Alzoubi. “AI-Driven Cybersecurity for Telemedicine: Enhancing Protection Through Autonomous Defense Systems.” In AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense, pp. 375-406. IGI Global Scientific Publishing, 2025.

24. del Moral, Javier Oliva, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, and Josu Etxezarreta Martinez. “Cybersecurity in critical infrastructures: A post-quantum cryptography perspective.” IEEE Internet of Things Journal 11, no. 18 (2024): 30217-30244.

25. Wahed, Mutaz Abdel. “AI-Enhanced Threat Intelligence for Proactive Zero-Day Attack Detection.” Gamification and Augmented Reality 3 (2025): 2.

26. Ko, Kyung-Kyu, and Eun-Sung Jung. “Development of cybersecurity technology and algorithm based on quantum computing.” Applied Sciences 11, no. 19 (2021): 9085.

27. Wahed, Mutaz Abdel, Mowafaq Salem Alzboon, Muhyeeddin Alqaraleh, Azmi Halasa, Mohammad Al-Batah, and Ahmad Fuad Bader. “Technological Innovations in Autonomous Vehicles: A Focus on Sensor Fusion

and Environmental Perception." In 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS), pp. 1-7. IEEE, 2024.

28. Jain, Aditya, Ligandro Singh Yumnam, and G. Usha. "Quantum Computing Cybersecurity—Exploring the Potential of Quantum Machine Learning Techniques in Intrusion Detection." In The Quantum Evolution, pp. 466-483. CRC Press.

29. Wahed, Mutaz Abdel, and Salma Abdel Wahed. "Assessing Internet Addiction Levels Among Medical Students in Jordan_ Insights from a Cross-Sectional Survey." International Journal of Advanced Health Science and Technology 5, no. 1 (2025): 12-18.

30. Alrashdan, Maen T., Mutaz Abdel Wahed, and Nader Mohammad Aljawarneh. "The Impact of Encrypted Data Confidentiality in the Accounting Management System Performance in terms of Employees' Passion and Customer Trust." International Journal of Advances in Soft Computing & Its Applications 16, no. 2 (2024).

31. Alrashdan, Maen T., Mutaz Abdel Wahed, Emran Aljarrah, Mohammad Tubishat, Malek Alzaqebah, and Nader Aljawarneh. "The impact of data recovery criteria, data backup schedule and data backup prosses on the efficiency of data recovery management in data centers." International Journal of Data and Network Science 8, no. 4 (2024): 2539.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Mutaz Abdel Wahed.
Formal analysis: Mutaz Abdel Wahed.
Research: Mutaz Abdel Wahed.
Methodology: Mutaz Abdel Wahed.
Project management: Mutaz Abdel Wahed.
Software: Mutaz Abdel Wahed.
Supervision: Mutaz Abdel Wahed.
Writing - proofreading and editing: Mutaz Abdel Wahed.