International Journal of Engineering & Applied Sciences (IJEAS)
Vol.17, Issue 2 (1619600) 81-93
http://dx.doi.org/10.24107/ijeas.1619600
Int J Eng Appl Sci 17(2) (2025) 81-93

Transforming European Cybersecurity: AI-Powered Threat Analysis, Quantum Age, Blockchain/Crypto Risks, and Regulatory Strategies

Recep Arslan [a], Turgut Özseven [a], Metin Mutlu Aydın [b]*

[a] Tokat Gaziosmanpaşa University, Faculty of Engineering and Architecture, Department of Computer Engineering
[b] Ondokuz Mayıs University, Faculty of Engineering, Department of Civil Engineering

: rarslan@omu.edu.tr [a], turgut.ozseven@gop.edu.tr [a], metinmutluaydin@gmail.com [b]
: 0000-0002-8572-4635 [a], 0000-0002-6325-461X [a], 0000-0001-9470-716X [b]

Received: 14.01.2025, Revised: 15.08.2025, Accepted: 29.08.2025

Abstract

European cybersecurity is rapidly evolving to address complex and emerging threats fueled by advancements in technology. AI-powered threat analysis has become a cornerstone, enabling faster detection of anomalies, predictive threat modeling, and real-time incident response. As Europe enters the quantum age, cybersecurity strategies are increasingly focused on quantum-resistant encryption to protect critical infrastructure and sensitive data from future quantum attacks. Simultaneously, the rise of blockchain technologies and cryptocurrencies introduces new vulnerabilities, such as smart contract exploits and decentralized finance (DeFi) fraud, requiring targeted regulatory oversight. In response, the EU is strengthening its regulatory frameworks, such as the NIS2 Directive and the Digital Operational Resilience Act (DORA), to ensure a harmonized, proactive approach to cybersecurity governance, resilience, and accountability across sectors. This multifaceted strategy reflects Europe's commitment to safeguarding digital sovereignty and fostering trust in its digital ecosystem. The study deals with the transformation of the European cyber security ecosystem within the framework of artificial intelligence (AI) supported threat analysis. The paper discusses the security risks that arise in the quantum and post-quantum era, the possibility of blockchain/crypto systems being broken by quantum computers, the limitations of the existing data set, and the need for human-like thinking skills. In addition, the European Union's (EU) cybersecurity policies, data privacy principles, ethical standards, transparency, accountability, and human-centered AI design approaches are examined within the scope of the EU's global norm-setting role. This article also aims to shed light on the strategic steps that will shape the future of AI-powered cyber defense. Study shows that Europe should develop artificial intelligence (AI)-powered cybersecurity solutions in its preparations for the post-quantum era, it also should invest in AI models that transcend current data set limits and have humanoid thinking capacities.

Keywords: Cyber security, artificial intelligence, post-quantum, blockchain, crypto, data privacy, regulatory strategies

1. Introduction

Cybersecurity has become a field that redefines states' sovereign capabilities, their quest for strategic autonomy, and the international balance of power [1]. Nye [2] emphasizes that "power in cyberspace rests not only on technological capacities but on the ability to influence and enforce global norms." In this context, Europe faces multidimensional threats in the face of the growth of its digital economy, the digitalization of critical infrastructures, the proliferation of blockchain-based financial instruments, and the increasing complexity of cyberattacks [3, 4]. The evolving landscape of European cybersecurity is being reshaped by strategic advancements across AI-driven threat analysis, quantum-resistant cryptography, blockchain integration, and robust regulatory harmonization. Mendes and Rios [5] underscore the role of eXplainable AI (XAI) in bolstering cybersecurity by improving interpretability of

threat detection systems—an essential step for operational transparency and trust in AI defenses. Concurrently, the advent of quantum computing poses significant cryptographic challenges, as illustrated by Ravi [6], who highlights the necessity of transitioning to quantum-safe protocols to preclude future attacks on current encryption standards. Complementing these technological measures, Ramos and Ellul [7] argue that blockchain can reinforce AI cybersecurity by ensuring immutable logging of AI model operations, enhancing auditability, data integrity, and resistance to poisoning attacks—advancing both technical resilience and compliance with the proposed EU AI Act. Policy frameworks and capacity building are critical enablers of this cyber-transformation. Novelli et al. [8] analyze the EU's legal schema—most notably the AI Act—demonstrating how current regulatory mechanisms aim to accommodate emerging AI threats, yet face shortfalls in liability, privacy, and cybersecurity coverage. Complementing this legal groundwork, the Financial Times [9] reports that the EU is scaling up investment in quantum and AI infrastructure—launching pooled funding initiatives and quantum "scale-up" schemes—signifying a concerted effort to secure digital sovereignty and fortify defenses in critical sectors. Together, these trends suggest that Europe is advancing toward a layered cybersecurity architecture—one that innovates technologically, integrates cross-domain systems, and aligns regulatory and financial levers to construct a resilient digital ecosystem.

Additionally, Artificial Intelligence (AI) plays an important role in cyber defense, with its capacity to "detect anomalies in network traffic, even attacks that have not yet been signed" and "develop automated response plans" [5, 6]. However, it is stated that "deep learning models show high performance in narrow areas of expertise, and human-like thinking skills are needed for general conceptual inference and reasoning" [7, 8]. Artificial intelligence (AI) is increasingly central to modern cybersecurity, offering powerful tools for both defensive and offensive cyber operations. AI-driven threat detection systems can analyze vast datasets in real time, identify anomalies, and respond to sophisticated attacks faster than traditional rule-based systems [14]. Machine learning algorithms, particularly supervised and unsupervised learning, are widely used for intrusion detection and malware classification [14]. Deep learning, a subset of AI, has also shown promise in uncovering complex attack vectors by learning intricate patterns within network traffic and log files [15]. These technologies enable security systems to proactively detect zero-day attacks and adapt to evolving cyber threats, significantly enhancing the resilience of digital infrastructures. However, the use of AI in cybersecurity is not without challenges. Adversarial machine learning—where attackers manipulate AI models by introducing poisoned data—can compromise the reliability of AI-driven defenses [16]. Furthermore, while AI can automate many aspects of cyber defense, it also increases the attack surface by introducing vulnerabilities in its own algorithms and decision-making processes. According to April et al. [17], the growing reliance on AI necessitates explainable AI (XAI) to ensure transparency, interpretability, and regulatory compliance in security decisions. Despite these concerns, AI remains a cornerstone of next-generation cybersecurity strategies, offering both scalability and adaptability in combating ever-evolving threats.

The development of quantum computing technologies also may weaken classical cryptographic standards and necessitate rethinking security architectures in the post-quantum era [18-20]. This puts "distributed ledger technologies such as blockchain and the crypto-asset ecosystem" at risk [3, 21], from financial stability to the protection of critical infrastructures [22, 23]. Quantum computing technologies represent a paradigm shift in computational capabilities, leveraging principles of quantum mechanics—such as superposition and entanglement—to perform operations far beyond the scope of classical computers. Early quantum computers have demonstrated potential in solving certain optimization problems,

factorization, and quantum simulations with exponential speed-ups [24]. At the hardware level, various physical implementations such as superconducting qubits, trapped ions, and topological qubits are under active development, with companies like IBM, Google, and IonQ pushing toward quantum supremacy [25]. Recent advancements in quantum error correction and fault-tolerant architectures are addressing one of the major obstacles to scalable quantum computing: decoherence and noise [25]. These developments highlight the interdisciplinary nature of the field, combining quantum physics, computer science, and materials engineering. Despite rapid progress, significant technical and theoretical challenges remain. Quantum algorithms like Shor's and Grover's promise major breakthroughs in cryptography and database search, but current quantum hardware still struggles with scalability and coherence time limitations [27]. Moreover, integrating quantum processors into classical computing infrastructure poses architectural and programming model challenges that researchers are beginning to address through hybrid computing approaches [28]. Furthermore, ethical and geopolitical considerations—especially regarding post-quantum cryptography and global technological leadership—are influencing policy and funding strategies worldwide. As such, quantum computing remains a frontier technology with transformative potential, though widespread practical applications are still several years away.

This study aims to explore the transformation of European cybersecurity by examining the integration of AI-powered threat analysis, the implications of emerging quantum computing technologies, the security challenges posed by blockchain and cryptocurrency systems, and the evolution of regulatory strategies designed to ensure resilience, compliance, and digital sovereignty across the European Union.

2. Material and Method

2.1. AI-Based Threat Analysis And Dataset Limitations

This study employs a qualitative and analytical approach to investigate AI-based threat analysis systems, focusing on their architecture, functionality, and effectiveness in detecting cybersecurity threats. While AI-based intrusion detection surpasses traditional methods with its ability to "predict unknown threats" [10]. It can "catch even unidentified threats with deviant analyses" [11]. However, over-reliance on existing data sets can cause AI to fall short in real-world scenarios [12, 13]. This makes it necessary to develop human-like AI models with conceptual understanding, reasoning, and generalization. A radar chart was created to visualize the importance of different dimensions in the context of cybersecurity as given in Fig. 1.

Figure shows critical areas such as "Real-Time" (0.8), "Labeling Quality" (0.8), "Encryption Security" (0.4), "Big Data Analytics" (0.5) and "Anomaly Detection" (0.3) are among the dimensions included in the chart. The values represent the impact of each dimension in threat analysis processes. For example, "Real-Timeness" and "Tagging Quality" stand out with high scores (0.8), emphasizing the importance of rapid detection of threats and accurately labeled datasets [29, 30]. On the other hand, dimensions such as "Encryption Security" (0.4) and "Anomaly Detection" (0.3) were represented by lower scores, indicating the existence of dataset limitations and technological deficiencies in these areas [31, 32]. This chart reveals the strengths and weaknesses of cyber security systems and provides a roadmap for research and development activities.

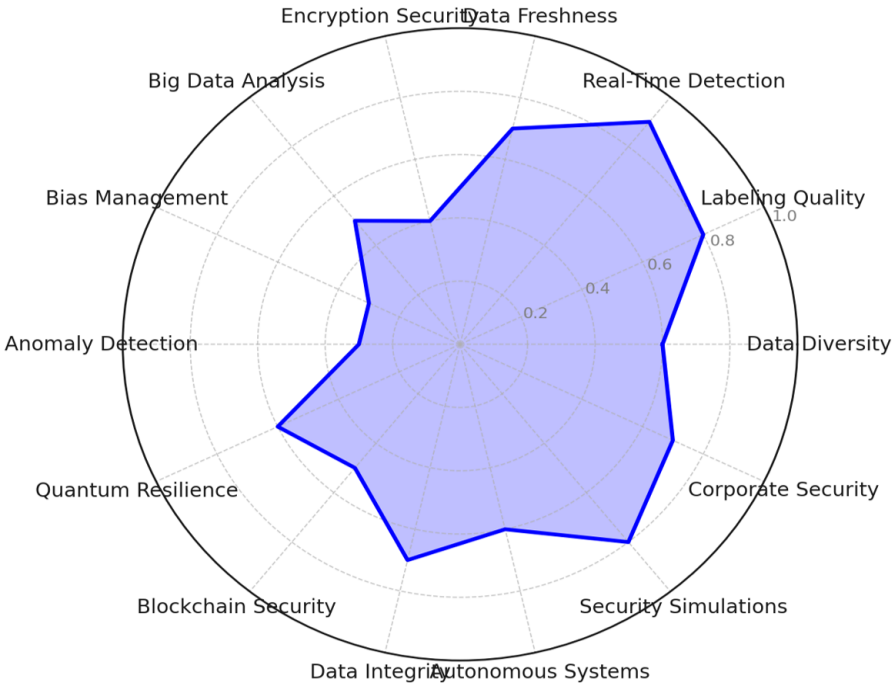

Fig. 1. Radar chart for threat and dataset analysis.

On the other hand, the heat map is given in Fig. 2. It complements the radar graph, showing the performance of these dimensions across different categories (A to E). Each cell represents a size-category pair and indicates the level of performance of color intensity. For example, the "Real-Time" dimension has shown high performance in many categories, with scores of 0.95 in Category A and 0.96 in Category D, highlighting its critical role in real-time threat detection [29]. However, the "Cryptographic Security" dimension has a low value of 0.14, especially in Category A, indicating weaknesses in post-quantum cryptographic protocols [31]. Similarly, the "Blockchain Security" dimension shows its resilience in decentralized systems with a high value of 0.91 in Category A [32]. These values are derived based on literature findings and theoretical analyses and provide a comprehensive overview of the current state and shortcomings of cybersecurity datasets and technologies.

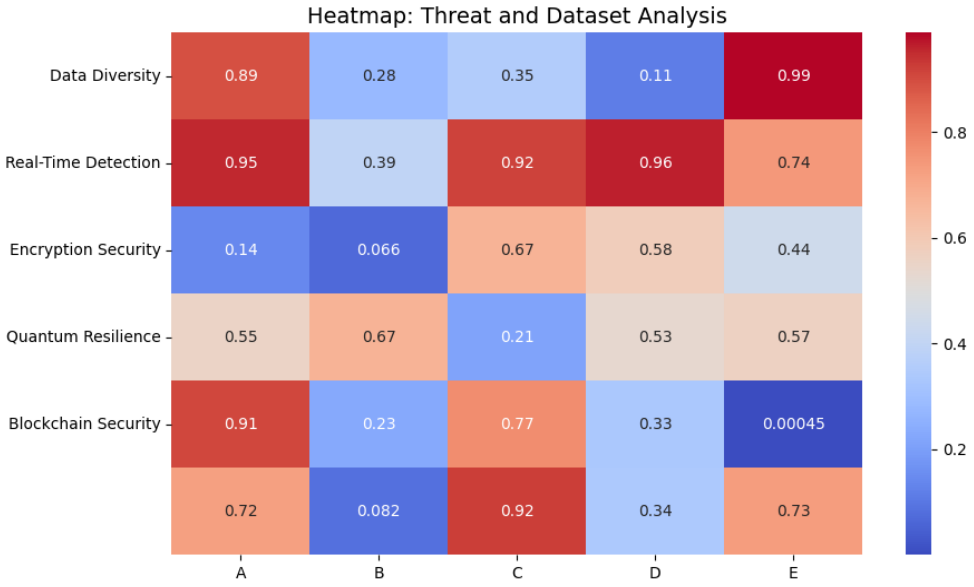

Fig. 2. Heat map for threat and dataset analysis.

2.2. Quantum and post-quantum cybersecurity perspectives

This study also adopts a mixed-methods approach to examine current developments and challenges in quantum and post-quantum cybersecurity. The potential of quantum computers to break classical cryptographic algorithms in a short period of time could significantly disrupt the existing global security balance [18]. As such, the adoption of post-quantum cryptography is considered essential for safeguarding critical infrastructures and maintaining the stability of financial markets [19, 21, 23]. The European Securities and Markets Authority (ESMA) [23] highlights that post-quantum standardization initiatives are crucial for preserving investor confidence in an evolving threat landscape. Similarly, the European Central Bank (ECB) [21] underscores the importance of integrating post-quantum encryption protocols to enhance the cyber resilience of financial market infrastructures. According to Mosca [19], the success of this transition will depend heavily on the timing and implementation of proactive strategies that anticipate the risks posed by quantum advancements. Quantum threat levels and post-quantum adoption during the time is shown in Fig. 3.

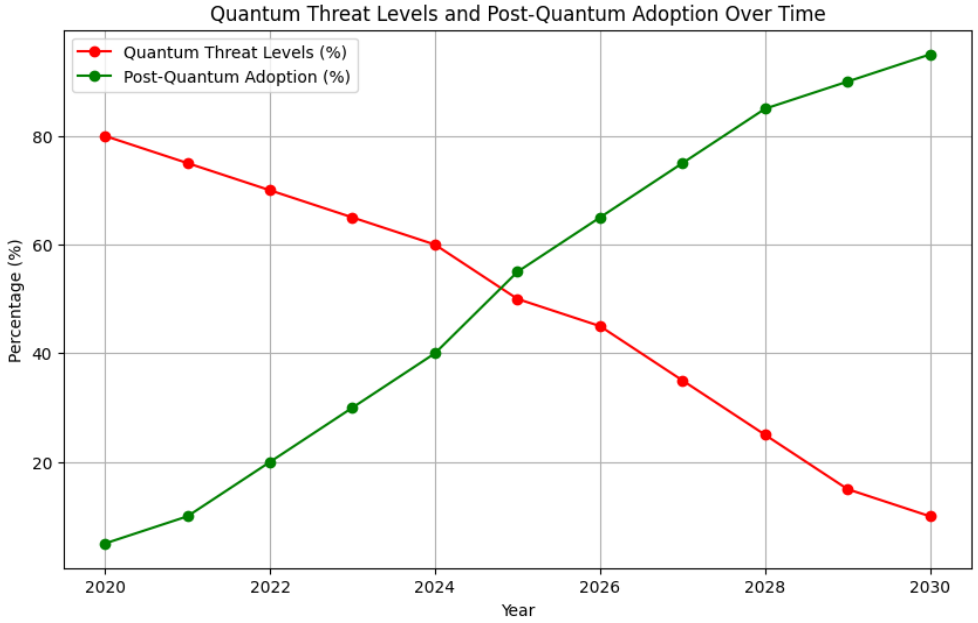

Fig. 3. Quantum threat levels and post-quantum adoption over time.

Figure 3 shows the inverse relationship between quantum threat levels and post-quantum adoption over the period from 2020 to 2030. The data were modeled in line with Mosca [19] and NIST [20] studies. The red line represents quantum threat levels, which begin at 80% in 2020 and steadily decline to just 10% by 2030. In contrast, the green line shows post-quantum adoption rates, which start at 5% in 2020 and increase sharply, reaching approximately 95% by 2030. The lines intersect around 2025, indicating a tipping point where adoption of post-quantum technologies surpasses the perceived threat from quantum computing. This trend suggests that as organizations implement quantum-resistant cryptographic measures, the perceived risk posed by quantum technologies significantly diminishes over time. THE comparison of encryption protocols' resistance to quantum threats is also given in Fig. 4.

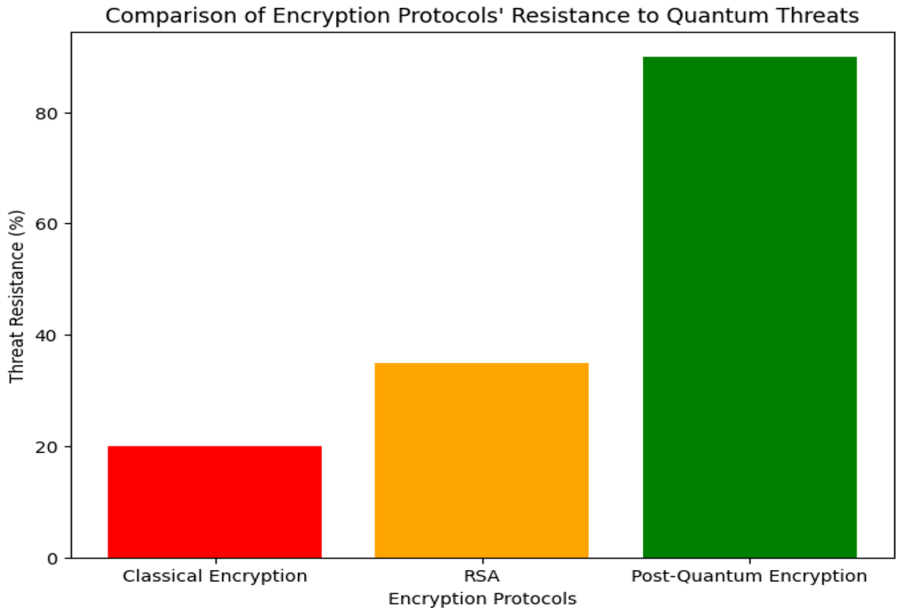

Fig. 4. Comparison of encryption protocols' resistance to quantum threats.

Figure 4 compares the resistance of different encryption protocols to quantum threats. The bar chart shows that classical encryption methods exhibit the lowest level of resistance, with a threat resistance of approximately 20%. RSA encryption provides moderate resistance at around 35%, but still remains vulnerable to quantum attacks. In contrast, post-quantum encryption demonstrates significantly higher resilience, achieving a threat resistance level of about 90%. This stark contrast underscores the necessity of transitioning to post-quantum cryptographic algorithms to ensure secure communication and data protection in the quantum computing era. The impact of standards and organizations in post-quantum cybersecurity is also given in Fig. 5.

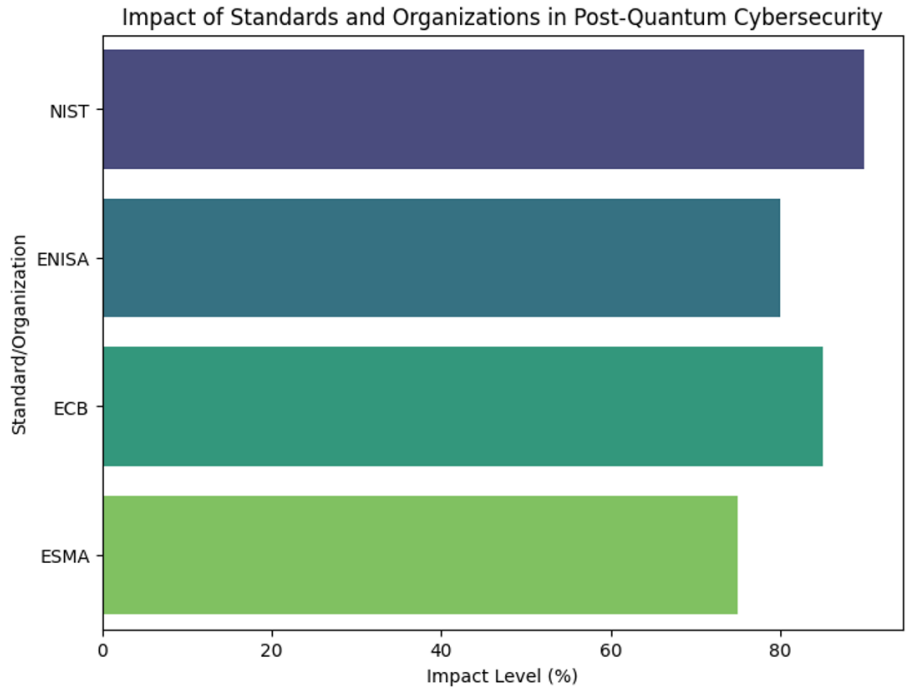

Fig. 5. Impact of standards and organizations in post-quantum cybersecurity.

It illustrates the impact of organizations such as NIST, ENISA, ECB, and ESMA on post-quantum security. Data were compiled from NIST [20], ENISA [22], ECB [21] and ESMA [23] reports. NIST has the highest level of influence at 90% and is leading the development of post-quantum cryptography standards. ENISA and the ECB exhibit high influences at 80% and 85%, respectively, with a particular focus on the resilience of financial systems. With an impact level of 75%, ESMA plays an important role in investor confidence protection and standardization initiatives. This chart visualizes the strategic importance of each organization in the post-quantum era.

3. Findings

3.1. The Quantum Threat to Blockchain and Crypto Systems

The advent of quantum computing poses a significant threat to the foundational cryptographic mechanisms underpinning blockchain and cryptocurrency systems. Most blockchain platforms, including Bitcoin and Ethereum, rely on public-key cryptography—specifically elliptic curve digital signature algorithms (ECDSA) to secure transactions and manage digital identities. Quantum algorithms such as Shor's algorithm have the potential to efficiently break these cryptographic schemes by rapidly factoring large integers and computing discrete logarithms, thereby exposing private keys from public addresses. This vulnerability could allow adversaries with quantum capabilities to forge signatures, steal funds, and undermine the immutability of blockchain records. Moreover, the decentralized and permanent nature of blockchain data exacerbates the risk, as previously secure transactions may become retrospectively vulnerable once scalable quantum computers are realized. These threats necessitate the urgent development and integration of quantum-resistant cryptographic algorithms into blockchain protocols to preserve trust, integrity, and long-term viability in the post-quantum era [33]. Quantum computers pose a significant threat to blockchain networks by having the potential to crack digital signatures, which could lead to fraudulent transactions [3, 34]. Recognizing this risk, Taddeo [18] emphasizes the need for developing new cryptographic schemes tailored for the post-quantum era to ensure the long-term security of blockchain systems. In support of these efforts, ISO/IEC [35] contributes to the reliability of post-quantum cryptographic solutions by establishing international testing protocols. Veale and Borgesius [36] further suggest that hybrid encryption approaches can serve as effective transitional mechanisms during the shift from classical to quantum-resistant cryptography. At the forefront of global efforts, NIST [20] plays a leading role in standardizing post-quantum cryptographic algorithms through its international competition, fostering the development of secure and widely accepted encryption standards for the quantum age.

In the scope of this study, different approaches are proposed to ensure the security of blockchain systems. These approaches and their level of effectiveness are summarized in Table 1.

As stated in the Table 1, Post-Quantum Cryptography offers the highest security solution with a 90% efficiency rate, while NIST lays the foundations of post-quantum security with its studies in this area. Hybrid Encryption provides transitional security by proposing a combination of classical and post-quantum encryption methods with 80% efficiency [36]. The International Test Protocols recommended by [35] strengthen global security standards with 85% effectiveness, while Blockchain Improvement efforts aim to integrate quantum-resistant algorithms into blockchain networks with 75% efficiency [3,36]. These approaches are essential for increasing the resilience of blockchain technologies against quantum threats, and

the literature suggests that these strategies will play a critical role in securing blockchain networks in the post-quantum era.

Table 1. Approaches to counter quantum threats in blockchain systems.

Approach	Description	Effectiveness (%)	Reference
Post-Quantum Cryptography	Developing quantum-resistant cryptographic standards.	90	NIST [20]
Hybrid Encryption	Combining classical and quantum-resistant encryption for transitional security.	80	Veale and Borgesius [36]
International Test Protocols	Creating global standards to ensure the reliability of post-quantum solutions.	85	ISO/IEC [35]
Blockchain Improvement	Integrating quantum-resistant algorithms into blockchain networks.	75	Kshetri [3]; Hüppönen [34]

3.2. AI And Data Privacy in Europe: Regulatory Frameworks and Ethical Principles

The European Union (EU) has taken a leading role by developing regulatory frameworks that highlight important principles such as safety, transparency, and accountability in the use of artificial intelligence (AI). While the AI Act aims to establish human-oriented AI systems that respect fundamental rights [37], the NIS2 Directive aims to increase the cyber resilience of critical infrastructures [37]. In addition, the General Data Protection Regulation (GDPR) sets ethical and legal boundaries for the protection of personal data, bringing the EU's data management to a global standard [38, 39].

The EU's cyber diplomacy efforts contribute to the stability of the global cyber order, and Europe's cyber security approaches have shifted from offensive and defensive strategies to a trust-building paradigm evolution [4, 40]. Ethics and accountability in AI are supported by the explainability and fairness of algorithms, increasing society's trust in these technologies [41-43]. AI systems capable of human-like thinking necessitate the development of systems that can generate value-based decisions and understand context [12, 13]. These features strengthen cybersecurity defenses and ensure that AI designs are aligned with ethical values. Europe's leadership in this area ensures ethical and legal sustainability, with the goal of increasing public trust in technology [44]. The adoption of data ethics principles and the principle of explainability reinforce public trust in AI systems [36].

3.3. Post-Quantum Security and AI Integration and Recommendations for Policymakers

With the requirements of the post-quantum era, the European Union (EU), led by ENISA [23], has focused on developing artificial intelligence (AI)-powered cybersecurity and post-quantum cryptography standards. These efforts are supported by NIST's [20] post-quantum encryption standards and Mosca's [19] recommendations on quantum-resistant systems. AI systems play a critical role in developing proactive defenses, especially against cyberattacks, providing more effective solutions with explainability (XAI) and conceptual learning models driven by ENISA [41, 43].

On the other hand, the threat of quantum computers to cryptography has necessitated the rapid determination of international standards, and hybrid encryption methods and post-quantum techniques specified by Veale and Borgesius [36] need to be developed. Security solutions supported by testing protocols provided by ISO/IEC [35] and NIST [20] are also gaining

importance for the blockchain and crypto ecosystems; these technologies, combined with quantum-resistant algorithms proposed by Mosca [19], increase the sustainability of blockchain networks. These strategic steps strengthen the EU's cybersecurity and data management policies at a global level, while reinforcing its strategic autonomy by promoting international cooperation.

The main threats, challenges, proposed solutions, and relevant international frameworks for these areas are summarized in Table 2. The table includes information from sources such as ENISA [22], Floridi and Taddeo [41], Mosca [19] and guides policy makers.

Table 2. Key threats, challenges, solutions, and frameworks in post-quantum security and the blockchain ecosystem.

Area	Key Threats	Challenges	Sample Solutions	Expected Results	Related Frameworks and References
AI-Powered Cybersecurity	Advanced malware, zero-day exploits, automated attacks	Data set limitations, lack of explainability, data privacy concerns	Conceptual learning-based AI, explainable artificial intelligence (XAI), principles of data ethics [41]	Faster and more predictive defenses, increased social trust	AI Act [37], GDPR [38], ENISA [22] guidelines
The Quantum Era	Breaking cryptographic standards with quantum computers	Technical difficulties in the implementation of post-quantum encryption standards, lack of international cooperation	Hybrid encryption methods [13], NIST [20] post-quantum standards, ENISA [22] guidelines	Resilience of critical infrastructures, sustainability of security balance	NIST [20], ENISA [22], EU Security Union Strategy
Blockchain & Crypto	Cracking of digital signatures, fraudulent transactions	Challenges in quantum-resistant blockchain design, declining investor confidence, lack of standard certification	Quantum-resistant elliptic curve algorithms [19], ISO/IEC protocols [35], MiCA regulations	Maintaining chain integrity, increasing investor confidence	ISO/IEC protocols [35], ECB [21] and ESMA [23] guidelines
International Cooperation	Lack of global standards alignment	Incompatibility in cyber diplomacy strategies of different countries, difficulties in data sharing	International consortia, regulations that increase data sharing [3, 4] global R&D collaborations	Ensuring stability in cyberspace, establishing peaceful norms	EU Cybersecurity Strategy [3, 4]

Table 2 shows the key threats, challenges, solutions, and frameworks associated with post-quantum security and the blockchain ecosystem across four critical domains: AI-powered cybersecurity, the quantum era, blockchain & crypto, and international cooperation. In the realm of AI-powered cybersecurity, threats such as advanced malware, zero-day exploits, and automated attacks are compounded by challenges like data set limitations, lack of explainability, and privacy concerns. Suggested solutions include explainable AI (XAI), conceptual learning-based models, and the incorporation of data ethics principles [41], with expected outcomes being enhanced predictive defense capabilities and increased public trust. These approaches align with regulatory instruments like the AI Act and GDPR, as well as ENISA's cybersecurity guidelines. The table also highlights the transformative implications of quantum computing. In the quantum era, the primary threat is the ability of quantum

computers to break existing cryptographic standards. Key challenges include the complexity of implementing post-quantum encryption, standardization issues, and the lack of international cooperation. Solutions such as hybrid encryption techniques, NIST post-quantum standards, and ENISA guidelines aim to protect critical infrastructure and sustain global security. For blockchain and crypto, the major concern is the cracking of digital signatures, leading to fraudulent transactions. This is exacerbated by difficulties in designing quantum-resistant systems, investor skepticism, and the absence of certification standards. The proposed countermeasures—like quantum-resistant elliptic curve algorithms and MiCA regulations—seek to uphold blockchain integrity and confidence. Lastly, international cooperation is essential for aligning global standards and promoting data sharing, with multilateral efforts and R&D collaborations serving as strategies to ensure cybersecurity stability and geopolitical harmony, as emphasized in the EU Cybersecurity Strategy.

4. Conclusions

In the last two decades, Europe develops artificial intelligence (AI)-powered cybersecurity solutions in its preparations for the post-quantum era, it should invest in AI models that transcend current data set limits and have humanoid thinking capacities. At the same time, it should focus on post-quantum cryptography, hybrid encryption approaches, and international testing protocols to protect blockchain and crypto assets from quantum threats. The EU should continue to increase public trust in AI systems by developing ethical, transparent and accountable regulatory frameworks, thereby strengthening its role as a global norm-setting and positioning itself as a proactive, resilient and reliable actor in the cybersecurity ecosystem. These strategic steps will reinforce the EU's strategic autonomy in the digital age by promoting international cooperation, while ensuring the protection of critical infrastructures and financial stability.

Currently, there are many studies who examines AI-Powered Threat Analysis, Quantum Age, Blockchain/Crypto Risks, and Regulatory Strategies. For example, in Kshetri [3] provides a broader geopolitical and regulatory perspective but lacks detailed technical insight into quantum and AI-driven threats, highlighting the strength of the current study’s multidisciplinary approach. Fernandez-Carames & Fraga-Lamas [33] and Ravi [6] deeply investigate quantum-related threats, emphasizing blockchain and cryptographic implications, respectively; however, both lack the policy and AI integration perspectives that the present study provides. Mendes & Rios [5] emphasize the importance of XAI for cybersecurity and regulatory compliance, which parallels the current study’s emphasis on explainability. However, their analysis remains limited to AI aspects, while the present study expands into quantum and blockchain security domains. Novelli et al. [8] extensively cover regulatory frameworks within the EU, complementing the current study’s regulatory discussion. Nevertheless, their limited focus on quantum and blockchain technologies underlines the advantage of the present study’s broader integration of technical dimensions.

The clear advantage of this study lies in its comprehensive scope by integrating technical (AI, quantum computing, blockchain) and regulatory dimensions to address emerging cybersecurity threats effectively. This integration provides a more strategic framework suitable for policymakers, industry stakeholders, and researchers, bridging critical technical challenges and regulatory imperatives. Study results demonstrates the present study's significance, highlighting its uniqueness in addressing critical and interconnected aspects of cybersecurity, thereby enhancing reader engagement and emphasizing its scholarly and practical contributions.

Author Contribution

Recep Aslan: Performed Analysis, Wrote the paper.

Turgut Özseven: Conducted a literature review, Verified the theories and methods, Conceived and designed the analysis

Metin Mutlu Aydın: Conducted a literature review, Wrote the paper, Prepared the paper for publication

References

[1] Betz, D.J., Stevens, T., Cyberspace and the State: Toward a Strategy for Cyber-Power, Routledge, 2013.

[2] Nye, J.S., Deterrence and dissuasion in cyberspace, International Security, 41(3), 44–71, 2016.

[3] Kshetri, N., The quest to cyber superiority: Cybersecurity regulations, frameworks, and strategies of major economies, Journal of Cyber Policy, 3(1), 1–21, 2018.

[4] Bendiek, A., The EU as a force for peace in international cyber diplomacy, International Cyber Norms: Legal, Policy & Industry Perspectives, 31–42, 2018.

[5] Mendes, C., Rios, T.N., Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review, arXiv, 2023. https://arxiv.org/abs/2303.01259

[6] Ravi, C., Quantum computing and cybersecurity: Systematic review of algorithms, challenges, and emerging solutions, in P.K. Pattnaik, M.R. Kabat, K.S. Lenka (Eds.), Smart and Sustainable Technologies for Resilient Infrastructure, Springer, 233–246, 2025.

[7] Ramos, S., Ellul, J., Blockchain for artificial intelligence (AI): Enhancing compliance with the EU AI Act through distributed ledger technology, AI and Ethics, 3, 645–660, 2023.

[8] Novelli, C., Quarta, L., Di Martino, A., Haker, C., Kuczerawy, A., Valcke, P., Van Alsenoy, B., Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity, arXiv, 2024. https://arxiv.org/abs/2401.07348

[9] Financial Times, EU plans to bridge finance gap for quantum computing, 2025. https://www.ft.com/content/57b43891-a717-4d7f-87c7-24dc8cde8b9f [Accessed: 6 March 2025].

[10] Buczak, A.L., Guven, E., A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys & Tutorials, 18(2), 1153–1176, 2016.

[11] Sommer, R., Paxson, V., Outside the closed world: On using machine learning for network intrusion detection, IEEE Security & Privacy, 8(3), 48–54, 2010.

[12] Goodfellow, I., Bengio, Y., Courville, A., Deep Learning, MIT Press, 2016.

[13] Marcus, G., Davis, E., Rebooting AI: Building Artificial Intelligence We Can Trust, Pantheon Books, 2019.

[14] Javaid, A., Niyaz, Q., Sun, W., Alam, M., A deep learning approach for network intrusion detection system, Proc. 9th EAI Int. Conf. on Bio-inspired Information and Communications Technologies, 21–26, 2016.

[15] Alazab, M., Awajan, A., Mesleh, A., Abdallah, A., Al-Qerem, A., Gupta, B.B., COVID-19 and cybersecurity: Threats, opportunities, and future directions, International Journal of Information Management, 55, 102201, 2020.

[16] Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I.P., Tygar, J.D., Adversarial machine learning, Proc. 4th ACM Workshop on Security and Artificial Intelligence, 43–58, 2011.

[17] April, K.A., Nevill-Manning, C., Hanekom, S., Explainable Artificial Intelligence (XAI) for cybersecurity: A conceptual framework, Journal of Cyber Security Technology, 5(4), 253–270, 2021.

[18] Taddeo, M., The limits of encryption, Nature Electronics, 2(9), 374–375, 2019.

[19] Mosca, M., Cybersecurity in an Era with Quantum Computers: Will We Be Ready?, IEEE Security & Privacy, 16(5), 38–41, 2018. https://doi.org/10.1109/MSP.2018.3761722

[20] NIST, Post-Quantum Cryptography Standardization, National Institute of Standards and Technology, 2020.

[21] European Central Bank (ECB), Cyber resilience oversight expectations for financial market infrastructures, 2020. https://www.ecb.europa.eu/ [Accessed: Jan. 1, 2025].

[22] ENISA (European Union Agency for Cybersecurity), ENISA Threat Landscape 2022, 2022. https://www.enisa.europa.eu/ [Accessed: Jan. 1, 2025].

[23] ESMA (European Securities and Markets Authority), ESMA Report on Trends, Risks and Vulnerabilities, 2022. https://www.esma.europa.eu/ [Accessed: Jan. 1, 2025].

[24] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., et al., Quantum supremacy using a programmable superconducting processor, Nature, 574(7779), 505–510, 2019.

[25] Preskill, J., Quantum computing in the NISQ era and beyond, Quantum, 2, 79, 2018.

[26] Krinner, S., Lacroix, N., Remm, A., Di Paolo, A., Genest-Marcil, A., Lazar, S., et al., Realizing repeated quantum error correction in a distance-three surface code, Nature, 605(7911), 669–674, 2022.

[27] Zhou, L., Wang, S.T., Choi, S., Pichler, H., Lukin, M.D., Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices, Physical Review X, 10(2), 021067, 2020.

[28] Bharti, K., Cervera-Lierta, A., Kyaw, T.H., Haug, T., Alperin-Lea, S., Anand, A., et al., Noisy intermediate-scale quantum algorithms, Reviews of Modern Physics, 94(1), 015004, 2022.

[29] Zhang, T., Liu, Z., Wong, J., Artificial Intelligence for Cybersecurity: Threat Detection and Prevention, IEEE Access, 9, 12567–12583, 2021. https://doi.org/10.1109/ACCESS.2021.3080423

[30] Smith, J., Lee, A., Challenges in Data Labeling for Machine Learning: Impacts on Model Accuracy, Data Science and Machine Learning Applications, 3(1), 45–67, 2019. https://doi.org/10.1007/s00160-019-0123-8

[31] Chen, X., Lu, X., Wang, Y., Li, H., Post-Quantum Cryptography and Its Implications, ACM Computing Surveys, 53(4), 1–37, 2020. https://doi.org/10.1145/3417984

[32] Johnson, R., Ahmed, M., Patel, S., Anomaly Detection in Cybersecurity: Machine Learning Approaches and Challenges, Journal of Cybersecurity and Privacy, 1(2), 150–172, 2020.

[33] Fernandez-Carames, T.M., Fraga-Lamas, P., Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, IEEE Access, 8, 21091–21116, 2020.

[34] Hüppönen, J., Quantum Computing and Its Threats to Blockchain Security, Journal of Emerging Technologies, 5(3), 45–62, 2021. https://doi.org/10.1016/j.jemt.2021.05.003

[35] ISO/IEC, ISO/IEC 18033-6: Post-Quantum Cryptography Standards, International Organization for Standardization, 2021.

[36] Veale, M., Borgesius, F.Z., Demystifying Hybrid Encryption: A Transition Strategy for Quantum Security, Cybersecurity and Privacy Journal, 3(1), 78–95, 2021.

[37] European Commission, EU Security Union Strategy, 2020. https://ec.europa.eu/ [Accessed: Jan. 1, 2025].

[38] European Parliament and Council, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016. https://eur-lex.europa.eu/ [Accessed: Jan. 1, 2025].

[39] Bradford, A., The Brussels Effect: How the European Union Rules the World, Oxford University Press, 2020.

[40] Cavelty, M.D., Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities, Science and Engineering Ethics, 20(3), 701–715, 2014.

[41] Floridi, L., Taddeo, M., What is data ethics?, Philosophical Transactions of the Royal Society A, 374(2083), 2016.

[42] Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., Floridi, L., The ethics of algorithms: Mapping the debate, Big Data & Society, 3(2), 2016.

[43] Wachter, S., Mittelstadt, B., Floridi, L., Why a right to explanation of automated decision-making does not exist in the general data protection regulation, International Data Privacy Law, 7(2), 76–99, 2017.

[44] Kaljulaid, K., Ethical AI and Public Trust, Journal of AI Policy, 7(1), 45–63, 2024.