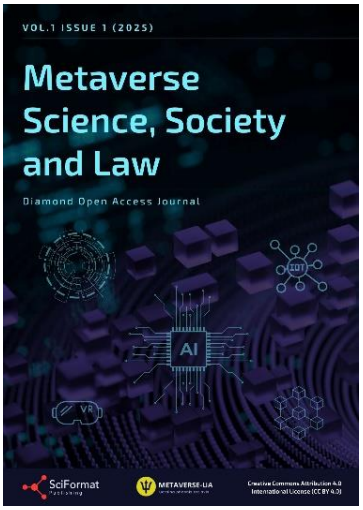

Metaverse Science, Society and Law

Vol. 1, Issue 1 (2025)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	QUANTUM SECURITY IN WEB 4.0: A NEW STAGE IN THE DEVELOPMENT OF THE METAVERSE
ARTICLE INFO	Danyila Oliinyk, Stepan Koshkarov, Yurii Konizhai. (2025) Quantum Security in Web 4.0: A New Stage in The Development of The Metaverse. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.16
DOI	https://doi.org/10.69635/mssl.2025.1.1.16
RECEIVED	24 April 2025
ACCEPTED	28 June 2025
PUBLISHED	24 July 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

QUANTUM SECURITY IN WEB 4.0: A NEW STAGE IN THE DEVELOPMENT OF THE METAVERSE

Danyila Oliinyk
Doctor of Economics, Professor, Chief Researcher at the Sectoral Economy Department, National Institute for Strategic Studies, Ukraine
ORCID ID: 0000-0001-8144-6482

Stepan Koshkarov
Candidate of Economic Sciences, Associate Professor, Lecturer in Economic and Computer Sciences, Chernivtsi Cooperative Professional College of Economics and Law, Ukraine
ORCID ID: 0009-0009-3597-5944

Yurii Konizhai
Bachelor of Arts in Business, Salzburg University of Applied Sciences, Ukraine
ORCID ID: 0000-0001-7854-2561

ABSTRACT

The rapid advancement of Web 4.0, or the Symbiotic Web, marks a pivotal shift in the evolution of the Internet, characterized by immersive digital experiences and intelligent, decentralized ecosystems. This paper explores the intersection of Web 4.0, the Metaverse, and quantum security, focusing on the urgent need to secure digital infrastructures against the growing threat of quantum computing. As the Metaverse becomes a dynamic driver of digital transformation and economic development, the integration of post-quantum cryptography and quantum-resistant systems is essential for ensuring data privacy, digital sovereignty, and cyber resilience. The study examines key technological trends - including AI, blockchain, XR, and the Industrial Metaverse - within the context of current geopolitical risks, particularly the war in Ukraine. It highlights international quantum strategies, post-quantum encryption standards, and emerging architectures such as quantum blockchain. The authors argue that a proactive approach to quantum security is imperative for safeguarding future virtual environments, emphasizing Ukraine's strategic opportunity to build a robust and ethical quantum ecosystem.

KEYWORDS

Web 4.0, Metaverse, Quantum Security, Post-Quantum Cryptography, Digital Sovereignty, Industrial Metaverse, Quantum Computing, Quantum Blockchain, XR Technologies, Data Privacy, Cybersecurity, Ukraine, Digital Transformation, Quantum Infrastructure

CITATION

Danyila Oliinyk, Stepan Koshkarov, Yurii Konizhai. (2025) Quantum Security in Web 4.0: A New Stage in The Development of The Metaverse. *Metaverse Science, Society and Law*. Vol. 1, Issue 1. doi: 10.69635/mssl.2025.1.1.16

Introduction.

Web 4.0, also known as the Symbiotic Web, is conceptualized in the scientific literature as the next generation of the Internet, in which integrated and interacting digital and real-world objects and environments create a highly engaging user experience [1]. The evolution of the Internet into a digital ecosystem has witnessed significant growth in interest since late 2021, particularly following Facebook's rebranding as Meta and the widespread adoption of the term "Metaverse" [2]. According to McKinsey & Company, the Metaverse is defined as an evolving digital space enabled by three-dimensional (3D) environments that employ virtual and augmented reality, along with other advanced Internet technologies [3]. These virtual worlds enable users

to disconnect from the physical world and engage with content in an immersive, scalable, synchronous, and persistent environment, thereby providing a heightened sense of telepresence [4].

On Web 4.0 platforms, it is possible to create a space for secure and personalized interaction with web applications and services [5]. It is considered that Web 4.0 or webOS will function in parallel with the human brain as an operating system in a network of highly intelligent interactions in the next stage of Internet development [6], which will combine existing technologies such as artificial intelligence (*AI)*, digital twins, blockchain, as well as augmented, mixed and virtual reality [7].

The characteristics that define Web 4.0 at this stage of development are: a decentralized ecosystem based on the blockchain infrastructure of Web 3.0 and giving users greater control and ownership of their data; AI-based autonomy, which can optimize decentralized governance by managing token economies or voting systems without human intervention; an immersive and spatial Internet, where Web 4.0 will integrate 3D environments, augmented *(AR)* and virtual reality *(VR)* to create a more engaging Internet; empowering users, especially in terms of identity management *(Self-sovereign identity, SSI)* and post-quantum security, which ensures that decentralized systems remain protected even from the most advanced computing threats. In this context, the Metaverse emerges as a dynamic innovation platform of numerous online communities and users, which helps to rethink interaction with the world around us and can lead to an acceleration of the transformation of the digital economy and the digital sovereignty of the state. The immersive and interactive features of virtual worlds are one of the main driving forces of the evolution from Web 3.0 to Web 4.0 in various sectors of the economy, which necessitates the implementation of security and privacy protection measures . [8].

Russia's full-scale invasion of Ukraine in February 2022 requires a radical rethink of the risks and threats to economic security, with increased support for Ukraine's digital and post-quantum security. The issue of post-quantum security is one of the defining topics of scientific research and development, which will ensure data protection in the future, where quantum computers become a reality, capable of breaking almost all public key schemes currently in use. Scientists define military quantum security as a dynamic new socio-legal category of scientific research that reveals global threats of cybermodernity and requires detailed study [9]. It is predicted that quantum technologies, due to their potential, represent the phenomenal digital communication in modern information wars of the 21st century that foreshadows cardinal changes in the conditions of warfare. Therefore, regardless of the actual time of the advent of the era of quantum computing, scientists are already faced with the task of preparing information security systems to resist quantum computing (*QC).*

The evolution of the paradigm from Web 3.0 to Web 4.0, based on numerous models, technologies, and social relationships, represents a transformative concept for integrating the physical and digital spheres and promotes the development of new technologies and their interaction, such as the Internet of Things (IoT), big data analytics, cloud computing, AR and VR, distributed ledger technologies (DLT), robotics, additive manufacturing, and quantum computing (QC). This paradigm shift is based on global access to information through computer networks, which play a crucial role in various spheres of life to ensure cybersecurity based on the implementation of cyber-physical systems (CPS). Consequently, increasing attention is being paid to network security in the context of achieving a high level of security for network and information systems (NIS) under the EU Directive on NIS. [10].

The Global Governance of Web 4.0 (Web4Hub) [11] is being considered by the European Commission in the context of the strategy for shaping Web 4.0 and virtual worlds through the implementation of the pilot project “Space for the Metaverse – Virtual World and the transition to Web 4.0” as one that adds the use of innovative technologies and reliable blockchain transactions to provide an intuitive, immersive experience [12]. In the European Commission’s report on the prospects for the development of the EU economy after 2030, it is noted that the global market for virtual worlds will grow from €27 billion in 2022 to over €800 billion by 2030 [13]. At the same time, it is emphasized that the integration of Web 4.0 applications still poses numerous challenges, especially related to the integration of AI agents capable of operating in decentralized infrastructures, which play a key role in providing network intelligence [14]. The Council of Europe's Digital Agenda for 2022-2025 points to the Metaverse as a development that poses both complex challenges and significant threats. A published report by Deloitte states that the foundation of the Metaverse is the continuous optimization of users' digital life experiences and knowledge through Extended Reality (XR) and the continuous iteration of XR technologies and equipment [15]. In this context, the term Extended Reality encompasses various technologies that create interactive environments by combining the real and virtual worlds, or by complete virtualization, which includes virtual reality (VR), augmented reality (AR), and mixed reality (MR).

As a result of the transition from Industry 4.0 to Industry 5.0, technological progress enhances the interaction between humans and machines and supplements real capabilities through the interactive visualization modes provided by Metaverse technology. The results of a systematic literature review indicate that Metaverse technologies, primarily AR and VR, have become powerful tools in manufacturing [16]. The Industrial Metaverse and Generative Artificial Intelligence (Generative AI, GenAI) are seen as a new trend ushering in a new era in the industrial digital landscape: real-time 3D visualization technologies (RT3D) with shared immersive RT3D applications, assets, and services. For example, Siemens has announced the launch of the AI-based "Industrial Metaverse" initiative, which aims to accelerate innovation and increase resilience, enabling solutions to key problems in entire industries [17]. This is also facilitated by the Pentagon's "SKYblue" initiative, which helps create databases for situation analysis and use AI in financial and personnel management systems, taking into account possible risks and forming a "military laboratory of the future," which allows for storing data in a secure, distributed network, as well as interacting and creating innovative applications and services through the use of smart contracts.

According to a Meticulous Research report, published in June 2025, the industrial Metaverse market is experiencing extraordinary growth. Its market valuation is projected to grow from US$48.2 billion in 2025 to an expected US$600.6 billion by 2032, representing a compound annual growth rate of 20.5% over the forecast period [18]. The growth of the industrial Metaverse market expansion reflects the rapid adoption in many sectors of the economy of immersive digital technologies that merge physical and virtual environments, particularly in manufacturing, engineering, and operational processes, and create a new stage for the formation of effective innovative business models.

According to forecasts, the integration of XR technologies creates exciting industrial environments, while cloud computing and AI integration improve scalability to support industry competitiveness and drive innovation. The key players in the industrial Metaverse security market are currently leading companies such as Oracle Corporation, Microsoft, NVIDIA, IBM, Cisco Systems Inc. in the USA, Arm Limited in the UK, ABB Ltd. in Switzerland, Siemens AG, Robert Bosch GmbH, SAP SE in Germany, as well as industrial software and hardware suppliers such as Dassault Systèmes SE in France [19].

At its core, the Industrial Metaverse is a digital ecosystem where physical assets, manufacturing processes, and supply chains are reflected as virtual twins, which allow organizations to model, control, and optimize industrial operations in real time and achieve a growth of US$150 billion for the Industrial Metaverse by 2035, according to predictions by GLOBE NEWSWIRE [20]. However, this process is complicated by the full-scale invasion of Ukraine by the Russian Federation, which necessitates joint decisions regarding the inclusion of quantum technologies in dual-use goods and qubit circuits that contain or support physical qubit networks under the Wassenaar Arrangement, in which countries agree to maintain transparency in the export of conventional arms and dual-use goods [21]. Such commitments place the issue of further development and implementation of quantum technologies at the center of the international community's attention. For example, the United States and China have already elevated quantum technologies to the level of global technological competition, where the product is a quantum computer, with the US focusing on computing and China on communications [22]. European countries are leaders in quantum technology research, with traditional European research strengths. Nobel laureate Anton Zeilinger [23] laid the foundation for the implementation of the European Quantum Communication Infrastructure (EuroQCI). The design, development, and deployment of EuroQCI is based on both a terrestrial segment (fiber-optic communication networks) and a space segment (satellites) [24]. In fact, the EU recommendations concern the need for a coordinated approach to Europe's transition to a quantum-secure digital infrastructure [25], while the G7 cybersecurity expert group emphasizes combating the risks to the financial sector associated with quantum computing [26]. The International Telecommunication Union is also considering the issue of strengthening global digital cooperation to build a more inclusive and sustainable information society by establishing international technological standards [27].

Currently, leading countries worldwide are working on long-term joint research projects that will enable the practical application of quantum computers in the future, both in terms of hardware and software. For example, Japanese companies Fujitsu and RIKEN plan from 2025 to 2029 to provide large-scale quantum computers to global companies and research institutions for joint research in various fields, including finance.

In essence, large-scale quantum computers are currently largely experimental and pose risks to existing cryptographic protocols used to protect data in the Metaverse. In addition, quantum computers are extremely sensitive to noise and interference, which is a serious limitation to their widespread adoption and will require

millions of qubits that can operate without errors indefinitely. Furthermore, any two-level quantum system can be used as a qubit.

Scientists are currently developing various methods for quality control of post-quantum cryptography (PQC), which allows systems to remain protected even from the power of quantum computing. New encryption algorithms to protect against quantum computer attacks are now laid out in the initial set of quantum-resistant encryption standards from the US National Institute of Standards and Technology (NIST) and initiated by financial institutions to assess the risks of quantum computing within their areas of responsibility [28].

To protect the integrity of the Metaverse, the implementation of quantum-resistant cryptography is becoming essential. Recently, the most common methods for protecting against quantum computer attacks include Quantum Key Distribution (QKD), a technology that uses the laws of quantum mechanics to ensure security, unlike classical methods that rely on the computational complexity of mathematical problems. Scientists Sun, S., and Huang, A., while assessing the security of a practical quantum key distribution system, concluded that there is a need for analyzed and controlled parameters for certain quantum hacking strategies [29]. However, as the scientists note, establishing thresholds for these security parameters remains an open issue in practice, as a general security model that includes all parameters is still unavailable [30].

Scientists are continuing research into high-performance discrete-modulation and continuous-variable quantum key distribution over long distances (CV-QKD) [31], multi-particle entanglement in noisy quantum networks [32], routing schemes for quantum key distribution in hybrid-trusted QKD network systems [33], security analysis for practical quantum key distribution with arbitrary encoding schemes [34], quantum information processing based on quantum blockchain architecture [35], and more.

Scientists consider the development of new classical cryptographic algorithms, so-called post-quantum cryptography (PQC), to be resistant to attacks from future quantum computers. In 2024, NIST approved the first post-quantum cryptography standards-CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+-which form the basis for secure communications in the post-quantum era [36]. Modern cryptographic security protocols that provide secure communication channels over a network (e.g., SSL and TLS) rely on public-key algorithms that can be easily broken by powerful quantum computers using Shor's quantum factorization algorithm, which allows for factoring a number in polynomial time using logical qubits [37].

The implementation of post-quantum encryption algorithms to replace traditional encryption methods is a particularly important step in ensuring the protection of confidential information from potential threats in an era of rapid technological development. As a result, quantum computing has made significant progress in demonstrating quantum advantages over the past decade [38]. For instance, physicists at the University of Oxford conducted an experiment to create practical quantum computers that can solve specific problems regarding the precision of qubit control, which allows for reducing errors to 1 in 6.7 million [39]. Microsoft has also developed a new way to correct errors in quantum computing using innovative 4D encoding, which can improve the accuracy of quantum computing by a factor of 1000. IBM has announced the development of quantum error correction methods, which they predict will lead to the development of a demonstrably useful quantum computer by 2029 [40].

In essence, quantum security for building more reliable information protection and communication network systems - and for developing security measures - is based on the principles of quantum mechanics and their unique properties, such as superposition, entanglement, and uncertainty, to counter both traditional and quantum attacks. On the one hand, this poses threats to current cryptographic foundations, including those of Web 4.0. On the other hand, it offers unprecedented opportunities to create entirely new information security methods, which requires legislative and regulatory action to accelerate the implementation of post-quantum cryptography and the modernization of IT systems-both of which play a critically important role in ensuring economic security [41].

Science and technology megaprojects are a major component of long-term research and development plans for the creation and implementation of quantum computers, which requires the implementation of priority measures for the development of quantum science to shape the future Metaverse and a proactive approach to security and the development of new standards in the following directions:

- increasing computing power and data processing speed, which will allow for the creation of much more complex, realistic, and interactive virtual worlds, simulations, and practical experiences;
- accelerating and improving AI and machine learning algorithms, which will allow for the creation of realistic avatars and non-player characters;
- creating accurate models of physical processes, chemical reactions, and biological systems, which can be used for medical simulations, engineering design, and scientific research in virtual space;

- developing quantum-resistant blockchain solutions for decentralized ownership and secure transactions in the Metaverse;

- increasing the level of user immersion in the Metaverse based on quantum technologies that could potentially impact sensory and other interfaces;

- providing access to quantum computing through cloud platforms, allowing for rapid prototyping and testing of ideas without the need to purchase expensive equipment.

Recent studies show that the number of qubits needed to break traditional encryption has dramatically decreased from 1 billion in 2012 to only 1 million in 2025. Experts predict that by 2030, quantum computers will be able to decrypt current encrypted Internet traffic [42]. While quantum-enhanced authentication methods can significantly improve the security of endpoints and IoT devices, as an integral part of Web 4.0, this process will require a major upgrade of existing systems, protocols, and security standards that underpin metadata.

Despite its significant advantages, quantum security currently faces challenges. Among the most significant are:

- transition and coordinated implementation to post-quantum cryptography by the end of 2026 according to the recommendations and the EU roadmap for the transition to PQC [43];

- long-distance transmission of quantum keys remains challenging, which is a technological limitation for global scaling for all types of data [44];

- building and maintaining a quantum data transmission infrastructure, especially in cloud environments, requires special fiber optic cables, quantum repeaters, and equipment where each photon is transmitted individually, which slows down the process. The transition to PQC also poses significant financial challenges. For comparison, the US federal government's migration to PQC between 2025 and 2035 is estimated to cost approximately $7.1 billion [45];

- lack of visibility of cryptographic assets, which makes it difficult to determine the need for their update.

Web 4.0 contains a huge number of documents where confidentiality and security are crucial for big data. As experts note, 90% of the world's digital data has been generated in the last two years, and the volume of data grows by 50% every year [44]. Data is the basis for forecasting, planning, and adjusting information that underlies combinations and visualizations on the Internet. The digital transformation of Ukraine's economy means a transition to an economic model centered on digital data and network transactions as primary resources and tools. AI-based predictive analytics, which is now being integrated into Metaverse platforms thanks to the availability of data and complex algorithms (natural language processing, computer vision, generative AI, etc.), currently allows for the analysis of large volumes of data and the improvement of present-day conceptual decision-making.

The presence of big data in the Metaverse means a change in traditional measurement methods in three different aspects: the amount of data (volume), the speed of data generation and transmission (velocity), and the heterogeneity of structured and unstructured data types (variety) [45]. The basis of such a statistical dataset is a set of observed values formed by a group of dimensions, along with associated metadata. To exchange statistical data in practice, the Data Cube Vocabulary is used, according to the standard of the Global Initiative for improving the exchange of statistical data and metadata (SDMX) [46], which allows representing such information using the semantic web with a Resource Description Framework (RDF) from a multidimensional perspective. The Data Cube Vocabulary is the foundation that supports extended vocabularies, which allow for the publication of statistical data streams or other multidimensional datasets [47]. Thus, information is stored in a data warehouse in the form of multidimensional cubes that are interactively queried for real-time decision-making (online analytical processing, OLAP) [48]. Despite the fact that analytical AI is widely implemented in various sectors of the economy, generative artificial intelligence remains in the early stages of implementation [49].

However, big data in the Metaverse increases the scale of problems related to confidentiality and security, and adds new ones that must be addressed through various methods and measures [50]. In this regard, research into the specific impacts of quantum technologies on changes in the real economy is gaining more substantive understanding, as it is a condition for ensuring quantum security in the Metaverse from the standpoint of advancing towards a quantum economy and intensifying these processes for the future.

Qubits, as the fundamental units of quantum information, are the basic building blocks of quantum computing, and the construction of quantum computers begins with the implementation of physical qubits. Physical qubits are inherently prone to errors and noise, making error correction essential for preserving the integrity of quantum information using “logical” qubits [51].

Recently, the experimental implementation of logical qubits has been demonstrated on leading quantum platforms, such as superconducting qubits, trapped ions, and neutral atom arrays [52]. The results of these experiments have shown significant potential for the realization of medium-scale logical quantum information processors with logical qubits in the near future. However, due to the limitations of current quantum computing systems, the development of fully fault-tolerant quantum computers requires significant efforts to ensure security in various areas, particularly in the hardware aspect of qubits.

To provide enhanced protection against future quantum attacks, scientists propose applying the potential of the quantum blockchain on a specialized Metaverse platform [53]. This approach is based on multilateral spatial data exchange and authentication using Quantum Multilateral Secret Computation (QMSC), integrated with a quantum blockchain network, thereby creating a highly secure environment [54]. The exchange of secret information, as a key research area in this field, has demonstrated its effectiveness in numerous applications, such as privacy protection and digital forensics. These and other security issues regarding the principles of global governance for Web 4.0 and virtual worlds were the subject of discussion at the European Commission's High-Level Global Multi-Stakeholder Conference in March 2025, and will be taken into account in the 20-year review of the World Summit on the Information Society (WSIS+20) [55].

Thus, quantum science is simultaneously a source of both significant threats and limitless opportunities for the Metaverse. The successful development of this sphere will require a proactive approach to security and the development of new standards in shaping digital sovereignty as the ability to control national digital assets [56]. This, in turn, requires the creation of a shared ecosystem for the comprehensive study of the potential of quantum technologies and the development of a joint strategy for regulating their potential [57]. According to scientists' conclusions, quantum technologies already have significant potential for the development of the communications sector, increasing situational awareness, timing, navigation, modeling, simulation, computing, and more, which are embedded in the strategic documents of many countries. Examples of countries that have adopted regulatory documents governing the implementation of quantum technologies include the USA [58], China [59], the United Kingdom [60], Canada [61], Australia [62], Ireland [63], and NATO [64].

Conclusions.

In Ukraine, at this stage, only the implementation of an experimental project on declaring the conformity of complex information protection systems in information, electronic communication, and information-communication systems created using information security profiles [65] and the protection of information, electronic communication, information-communication, and technological systems [66] has been initiated. Adopting an effective quantum strategy for Ukraine as a model for future development is a critically important step toward achieving digital sovereignty in conditions of war and post-war recovery and creating a reliable, ethical, and inclusive quantum ecosystem. In wartime, this process is complicated, as specific threats and challenges are added that affect data security, quantum computing, sensing, and communication. Therefore, building an effective system of quantum security in the metaverse and developing effective strategies and methods to counter threats must be a priority for ensuring the state's quantum security. By addressing these issues, Ukraine can navigate the evolving digital landscape of the Metaverse while ensuring that data privacy and quantum security remain top priorities in its legal and technological development. To describe the conceptual model of quantum security in the Metaverse, a high-level architecture of a big data system can be used, which includes a set of elements that facilitate the definition of security requirements and allow for a better understanding of threats and vulnerabilities [67].

REFERENCES

1. GeeksforGeeks. (2025). Web 4.0 - Intelligent Web. URL: https://www.geeksforgeeks.org/web-4-0-intelligent-web/
2. Zuckerberg, M. Founder 's Letter. 2021. Available online:. URL: https://about.fb.com/news/2021/10/founders-letter/ (accessed on August 18, 2022)
3. What is the metaverse ? URL: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-metaverse
4. Imagine a digital world where virtual and physical merge, enhancing interaction and personalization. URL: https://www.netguru.com/blog/web-4-0
5. Understanding Web 4.0: The Future of an Intelligent Internet. URL: https://www.netguru.com/blog/web-4-0
6. Ron, Callari (2009), "Web4.0, Trip Down the Rabbit Hole or Brave New World?" URL: http://www.zmogo.com/web/web-40trip-down-the-rabbit-hole-or-brave-new-world/
7. Shaping Web 4.0 Bitkom's Feedback to the European Commission's Survey Shape Web 4.0. Virtual worlds & Web 4.0 governance. URL: https://www.bitkom.org/sites/main/files/2024-11/bitkom-stellungnahme-shaping-web-4-0.pdf
8. Governance of Web 4.0 and virtual worlds. URL: https://commission.europa.eu/get-involved/events/governance-web-40-and-virtual-worlds-2025-03-31_en
9. Military quantum security as institutional cyber computing in the administrative-legal regime. URL: https://knushop.com.ua/index.php?route=product/product&product_id=5334
10. Directive on security of network and information systems (NIS Directive). URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198
11. WEB4HUB: A space for the metaverse – Virtual world and the transition to Web 4.0. URL: https://digital-strategy.ec.Europe.eu/en/policies/web4hub
12. Questions and Answers: EU initiative on Web 4.0 and virtual worlds: A head start in the next technological transition. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3719
13. EU competitiveness beyond 2030: looking ahead on the occasion of the 30th anniversary of the Single Market. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1668
14. Towards Web 4.0: Frameworks for Autonomous AI Agents and Decentralized Enterprise Coordination. URL: https://www.researchgate.net/publication/391568470_Towards_web_40_frameworks_for_autonomous_AI_agents_and_decentralized_enterprise_coordination
15. Metaverse report - Future is here Global XR industry insight. URL: https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-whitepaper.html
16. CES 2024: Siemens delivers innovations in immersive engineering and artificial intelligence to enable the industrial metaverse. URL: https://press.siemens.com/global/en/pressrelease/ces-2024-siemens-deliv
17. Industrial Metaverse Market Size, Share, Forecast, & Trends Analysis by Technology (AR/VR, Digital Twin, Autonomous Robots, Cloud Computing, AI/ML, 5G/6G, Blockchain, IoT, Location Services, Edge Computing, Exoskeleton), Application, End-use Industry - Global Forecast to 2032. URL: https://www.meticulousresearch.com/download-sample-report/cp_id=6001
18. Industrial Metaverse Market to Surge from USD 48.2 Billion to USD 600.6 Billion by 2032 – Meticulous Research. URL: https://www-prnewswire-com.translate.goog/news-releases/industrial-metaverse-market-to-surge-from-usd-48-2-billion-to-usd-600-6-billion-by-2032---meticulous-research-302493647.html?_x_tr_sl=auto&_x_tr_tl=uk&_x_tr_hl=uk
19. The Global Industrial Metaverse Market 2025-2035: Immersive Tech, AI, and Digital Twins Drive $150 Billion Industrial Metaverse Boom by 2035. URL: https://www.globenewswire.com/news-release/2025/03/31/3052006/28124/en/The-Global-Industrial-Metaverse-Market-2025-2035-Immersive-Tech-AI-and-Digital-Twins-Drive-150-Billion-Industrial-Metaverse-Boom-by-2035.html
20. Vassenaarska domovlenist shchodo kontroliu za eksportom zvychainykh ozbroien ta tovariv i tekhnolohii podviinoho vykorystannia: uhoda № 998_177 vid 01.07.1996. URL: https://zakon.rada.gov.ua/laws/show/998_177#Text
21. Quantum Technologies and the Future of Learning. March 2025. URL: https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch
22. The Nobel Prize in Physics 2022 was awarded jointly to Alain Aspect, John F. Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science". URL: https://www.nobelprize.org/prizes/physics/2022/summary/
23. The European Quantum Communication Infrastructure (EuroQCI) Initiative. URL: https://digital-strategy.ec.Europe.eu/en/policies/european-quantum-communication-infrastructure-euroqci

24. Commission publishes Recommendation on Post-Quantum Cryptography. URL: https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography#:~:text=The%20Recommendation%20addresses%20the%20need,of%20protecting%20their%20digital%20infrastructures
25. G7 Cyber Expert Group recommends action to combat financial sector risks from quantum computing. URL: https://www.gov.uk/government/news/g7-cyber-expert-group-recommends-action-to-combat-financial-sector-risks-from-quantum-computing
26. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
27. Schmidt, A., Fellmer, U. (2005), A polynomial quantum algorithm for computing the unit group of a number field, Proceedings of the Thirty-Seventh Annual ACM Symposium on the Theory of Computation – STOC '05, New York: ACM, Symposium on the Theory of Computation, pp. 475–480
28. Quantum computational advantage using photons. URL: https://www.science.org/doi/10.1126/science.abe877
29. Supertochni kubity: v Oksfordi zmenshyly pomylky kvantovykh kompiuteriv do 1 na 6,7 mln. URL: https://itc.ua/ua/novini/supertochni-kubity-v-oksfordi-zmenshyly-pomylky-kvantovyh-komp-yuteriv-do-1-na-6-7-mln/
30. Microsoft improved precision quantum calculations 1000 times. URL: https://x.com/ITCUA/status/1937137920088936604
31. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator.URL: https://www.science.org/doi/10.1126/sciadv.adi9474
32. Distributing Multipartite Entanglement over Noisy Quantum Networks.URL: https://arxiv.org/abs/2103.14759
33. Hybrid Trusted Quantum Key Distribution Network Routing Scheme for Power Grid Environment.URL: https://ieeexplore.ieee.org/document/10941900
34. Numerical security analysis for practical quantum key distribution with arbitrary encoding schemes.URL: https://www.researchgate.net/publication/391925043_Numerical_security_analysis_for_quantum_key_distribution_with_partial_state_characterization
35. D-Wave Introduces Quantum Blockchain Architecture, Featuring Enhanced Security and Efficiency over Classical Computing.URL: https://www.dwavequantum.com/company/newsroom/press-release/d-wave-introduces-quantum-blockchain-architecture-featuring-enhanced-security-and-efficiency-over-classical-computing/
36. NIST Releases First 3 Finalized Post-Quantum Encryption Standards.URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
37. Enhanced Network Security Protocols for The Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution .URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11002706
38. Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography
39. Shor's Factorization Algorithm. URL: https://www.geeksforgeeks.org/shors-factorization-algorithm/
40. Quantum computers could crack your encryption by 2030! URL: https://medium.com/@cyberteckmaster/quantum-computers-could-crack-your-encryption-by-2030-9c8797573e0b
41. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
42. Huang, D. et al. Continuous-variable quantum key distribution over large distances by controlling excess noise. Sci. Rep. 6, 19201; doi: 10.1038/srep19201 (2016).
43. The time has come to address the post-quantum security threat. URL: https://www.cognizant.com/us/en/insights/insights-blog/exposing-the-security-risk-of-quantum-computing
44. What is Data? Science and why Ukraine needs data science. URL: https://itukraine.org.ua/shho-take-data-science-i-navishho-ukrayini-nauka-pro-dani/
45. Min Chen, Shiwen Mao, and Yunhao Liu. 2014. Big data: A survey. Mobile Networks and Applications 19, 2 (2014), 171–209
46. ISO 17369:2013 Statistics data and metadata exchange (SDMX). URL: https://www.iso.org/standard/52500.html
47. Visualizing RDF Data Cubes Using the Linked Data Visualization Model. URL: https://www.researchgate.net/publication/290585340_Visualizing_RDF_Data_Cubes_Using_the_Linked_Data_Visualization_Model
48. The RDF Data Cube Vocabulary. URL: http://www.w3.org/TR/vocab-data-cube
49. AI in Action: Beyond Experimentation to Transform Industry FLAGSHIP WHITE PAPER SERIES JANUARY 2025. URL: https://reports.weforum.org/docs/WEF_AI_in_Action_Beyond_Experimentation_to_Transform_Industry_2025.pdf
50. Quantum Computation and Quantum Information by Nielsen and Chuang.URL: https://www.academia.edu/41154803/Quantum_Computation_and_Quantum_Information_by_Nielsen_and_Chuang

51. An elementary review on basic principles and developments of qubits for quantum computing. URL: https://nanoconvergencejournal.springeropen.com/articles/10.1186/s40580-024-00418-5
52. Complete Self-Testing of a System of Remote Superconducting Qubits. URL: https://journals.aps.org/prl/abstract/10. 1103/nv7d-k3wr
53. A Survey and Comparison of Post-quantum and Quantum Blockchains.URL: https://arxiv.org/pdf/2409.01358
54. Leveraging quantum blockchain for secure multiparty space sharing and authentication on specialized metaverse platform.URL: https://www.nature.com/articles/s41598-024-74213-x
55. The invisible evidence: Digital forensics as key to solving crimes in the digital age. URL: https://www.sciencedirect.com/science/article/pii/S0379073824002147
56. Questions and answers on the EU Quantum Strategy. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_25_1683
57. WEF Quantum for Society 2024. URL: https://www.scribd.com/document/842943156/WEF-Quantum-for-Society-2024
58. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. URL: https://irp.fas.org/offdocs/nsm/nsm-10.pdf
59. Chinese Quantum Companies and National Strategy 2023 https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023
60. National Quantum Strategy. URL: https://assets.publishing.service.gov.uk/media/6411a602e90e0776996a4ade/national_quantum_strategy.pdf
61. Canada's National Quantum Strategy. URL: https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy
62. National Quantum Strategy Building a thriving future with Australia's quantum advantage. URL: https://www.industry.gov.au/sites/default/files/2023-05/national-quantum-strategy.pdf
63. Minister Harris launches Quantum 2030, Ireland's first national strategy for quantum technologies. URL: https://www.gov.ie/en/department-of-further-and-higher-education-research-innovation-and-science/press-releases/minister-harris-launches-quantum-2030-irelands-first-national-strategy-for-quantum-technologies/
64. Summary of NATO's Quantum Technologies Strategy https://www.nato.int/cps/en/natohq/official_texts_221777.htm
65. Pro realizatsiiu eksperymentalnoho proektu z deklaruvannia vidpovidnosti kompleksnykh system zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh, stvorenykh z vykorystanniam profiliv bezpeky informatsii: postanova Kabinetu Ministriv Ukrainy vid 30 travnia 2024 r. № 627. URL: https://www.kmu.gov.ua/npas/pro-realizatsiiu-eksperymentalnoho-proektu-z-deklaruvannia-vidpovidnosti-kompleksnykh-system-zakhystu-informatsii-v-informatsiinykh-elektronnykh-komunikatsiinykh-i300524-627
66. Some issues of protection of information, electronic communication, information and communication, technological systems: Resolution of the Cabinet of Ministers of Ukraine No. 712-2025 dated 06/18/2025. URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-zakhystu-informatsiinykh-elektronnykh-komunikatsiinykh-informatsiino-s712180625
67. Global Multistakeholder High Level Conference on Governance of Web 4.0 and Virtual Worlds. URL: https://digital-strategy.ec.europa.eu/en/policies/event-web-4-governance