International Scientific Journal of Contemporary Research in Social Sciences and Humanities
2026 / No. 1 (1)
ELECTRONIC JOURNAL | OPEN ACCESS
Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

ARTIFICIAL INTELLIGENCE AND ECONOMIC SECURITY: EMERGING RISKS, GOVERNANCE CHALLENGES, AND RESILIENCE STRATEGIES

Atabayeva Ruhshona Sadulla qizi
Economics, Tashkent State University Of Economics

Abstract. Artificial intelligence (AI) is increasingly recognized as a general-purpose technology with significant implications for economic growth, employment, financial stability, and national security. This article examines how AI reshapes economic security, understood as the capacity of households, firms, and states to withstand shocks to income, markets, and critical infrastructure. Using a structured narrative review of academic research, international policy reports, regulatory frameworks, and technical safety studies, the article identifies four principal risk domains: labor-market disruption, market concentration and infrastructure dependence, financial instability, and malicious or geopolitical misuse. The review also examines governance challenges arising from fragmented regulatory approaches, limited institutional capacity, incomplete evidence, and the rapid pace of technological deployment. The findings indicate that AI-related risks are interconnected and that vulnerabilities can spread through shared models, concentrated computing infrastructure, and correlated institutional decisions. In response, the article proposes a layered resilience framework combining adaptive regulation, competition policy, financial supervision, workforce investment, and international coordination. It concludes that economic security depends not only on preventing harmful applications of AI but also on strengthening institutions' ability to anticipate, absorb, and recover from technological shocks.

Keywords: artificial intelligence, economic security, AI governance, financial stability, labor markets, resilience

International Scientific Journal of Contemporary Research in Social Sciences and Humanities
2026 / No. 1 (1)
ELECTRONIC JOURNAL | OPEN ACCESS
Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Introduction. Artificial intelligence (AI) has become an increasingly important factor in economic transformation. The public release of ChatGPT in late 2022 brought generative AI to widespread attention and accelerated debates about its potential to change employment, productivity, business operations, and public administration. AI systems can now support activities such as drafting documents, generating software code, analyzing financial information, and assisting with decision-making. These developments have created opportunities for productivity growth while raising concerns about economic dependence, unequal distribution of benefits, and systemic vulnerability.

The economic consequences of AI extend beyond the performance of individual firms or industries. As AI becomes integrated into financial services, supply chains, digital infrastructure, and public institutions, disruptions in one part of the technological ecosystem may affect many other organizations. An outage at a major cloud provider, for example, may interrupt services across several sectors. Similarly, the widespread adoption of similar AI models may create common vulnerabilities that are not immediately apparent when institutions assess risks independently.

This article approaches these issues through the concept of economic security. Because the term has no universally accepted definition, it is used here to describe the capacity of households, firms, and states to maintain stable incomes, functioning markets, and access to critical infrastructure during periods of disruption. This definition emphasizes both protection against immediate threats and the ability to adapt to structural economic change.

Previous research has examined AI's implications for productivity, employment, income distribution, and financial stability. Acemoglu (2024), for example, questions whether the near-term macroeconomic gains from AI will be as substantial as some forecasts suggest. Acemoglu and Restrepo (2019) explain how automation can displace workers while also creating new tasks. Meanwhile, the Financial Stability Board (FSB, 2024) identifies several channels through which AI adoption may affect the resilience of financial institutions and markets.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Despite these contributions, the relationship between AI and economic security requires an integrated perspective. Labor-market adjustment, technological concentration, financial interdependence, and malicious use are often examined separately, even though they can reinforce one another. Governance arrangements are also divided among institutions responsible for employment, competition, financial regulation, cybersecurity, and national security.

The purpose of this article is to synthesize the available literature on these interconnected issues and identify practical strategies for strengthening economic resilience. It addresses three research questions:

1. What are the principal risks that AI creates for economic security?
2. Why do existing governance arrangements struggle to address these risks effectively?
3. What policies can strengthen the capacity of economies and institutions to withstand and adapt to AI-related shocks?

The article argues that AI-related economic security depends not only on technological performance but also on the distribution of economic gains, the concentration of essential infrastructure, the degree of institutional preparedness, and the capacity for coordinated action. Because the evidence is still developing, the analysis distinguishes documented vulnerabilities from plausible risks that require further empirical investigation.

Methods.

Research Design

This article uses a structured narrative literature review to examine the relationship between artificial intelligence and economic security. A narrative approach is appropriate because the subject spans several disciplines, including economics, financial regulation, technology governance, cybersecurity, and international relations. These fields use different concepts and research methods, making a single quantitative synthesis difficult.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

The analysis focuses on identifying recurring risk mechanisms, comparing governance approaches, and synthesizing policy recommendations. It does not present original experimental data or claim to estimate the causal effects of AI adoption on economic outcomes. Instead, it develops an integrated analytical framework from previously published research and institutional assessments.

Sources and Selection Criteria

The review draws on four principal categories of sources.

First, it uses peer-reviewed economics research on automation, productivity, labor-market adjustment, and income distribution. Relevant contributions include Autor (2015), Acemoglu and Restrepo (2019), and Eloundou et al. (2024).

Second, the review considers reports from international institutions, particularly the International Monetary Fund (IMF) and the Financial Stability Board. These sources provide assessments of AI exposure across labor markets and identify potential vulnerabilities within financial systems.

Third, it examines technical research on foundation models, malicious uses of AI, and emerging safety concerns. The work of Bommasani et al. (2021), Brundage et al. (2018), and Bengio et al. (2025) informs the discussion of shared model dependencies, cybersecurity, fraud, and uncertainty surrounding advanced AI capabilities.

Fourth, the review considers governance frameworks and regulatory instruments, including the OECD AI Principles, the European Union AI Act, and the National Institute of Standards and Technology AI Risk Management Framework.

Sources were selected for their relevance to at least one of the following themes: economic and labor-market effects, market concentration and infrastructure dependence, financial-system vulnerabilities, malicious or geopolitical uses, and regulatory capacity. Particular attention was given to research that identifies mechanisms through which technological risks can spread beyond individual users or organizations.

This is a targeted narrative synthesis rather than an exhaustive systematic review. No comprehensive database search, formal screening protocol, or statistical meta-analysis is claimed. Consequently, the findings should be interpreted as a structured

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

synthesis of selected literature rather than a complete inventory of all published evidence.

Analytical Framework

The selected literature was organized into four risk domains: labor-market disruption; market concentration and infrastructure dependence; financial instability; and malicious or geopolitical misuse. These categories were chosen to connect individual economic effects with broader questions of systemic resilience.

Each domain was examined through three analytical dimensions:

Risk mechanism: How AI adoption may create or amplify economic vulnerability.

Governance gap: Why existing institutions, rules, or monitoring systems may be insufficient.

Resilience response: What policy or organizational measures may reduce exposure or improve recovery.

The analysis then compared the risk domains to identify common mechanisms, particularly technological concentration, information asymmetry, correlated decision-making, and uneven distribution of adjustment costs. These mechanisms provide the basis for the integrated policy framework presented in the Discussion section.

Results.

Labor-Market Disruption and Unequal Economic Adjustment

The literature indicates that AI exposure is widespread but unevenly distributed across occupations, sectors, and countries. The IMF estimates that nearly 40% of global employment is exposed to AI, with exposure reaching approximately 60% in advanced economies and around 26% in low-income countries (Cazzaniga et al., 2024). These figures describe potential exposure rather than the proportion of jobs certain to disappear.

Exposure can produce different outcomes. AI may complement workers by helping them complete tasks more efficiently, improve the quality of their output, or perform activities that previously required substantial time. In other cases, AI may reduce the demand for particular tasks, weaken workers' bargaining positions, or allow firms to

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

reorganize production with fewer employees. Eloundou et al. (2024) similarly find that large language models have the potential to affect a substantial proportion of tasks performed by workers in the United States.

The distinction between task exposure and job displacement is essential. Jobs consist of multiple activities, and the automation of some activities does not necessarily eliminate an entire occupation. Autor (2015) explains that technological change has historically transformed the composition of work while creating demand for tasks that require human judgment, interpersonal interaction, and contextual understanding.

Nevertheless, the pace and distribution of adjustment remain important concerns. Acemoglu and Restrepo (2019) distinguish between the displacement of labor by automation and the creation of new tasks in which human workers retain a comparative advantage. Economic outcomes depend partly on the balance between these forces. If displacement proceeds faster than the creation of new tasks, workers may face prolonged unemployment, wage reductions, or declining job security.

These effects may be particularly difficult for workers whose skills are closely tied to declining occupations or local labor markets with limited alternative employment. The benefits of AI may also accrue disproportionately to firms, investors, and highly skilled workers who can use or own the technology. Korinek and Stiglitz (2019) emphasize that technological progress can increase inequality when market outcomes do not adequately distribute its benefits.

The literature therefore identifies labor-market disruption as both a productivity issue and an economic security issue. Even if aggregate output rises, households may remain vulnerable when income losses occur faster than workers can retrain or find alternative employment.

Market Concentration and Infrastructure Dependence

The development and deployment of advanced AI require computing resources, data, specialized expertise, energy, and substantial financial investment. These requirements can create barriers to entry, particularly for organizations seeking to develop and operate frontier models. Bommasani et al. (2021) discuss the opportunities

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

and risks associated with foundation models, including the implications of building many downstream applications on a relatively limited set of general-purpose systems.

Concentration creates potential efficiency benefits. Large providers may spread development costs across many customers, maintain specialized security teams, and offer sophisticated infrastructure that smaller organizations could not build independently. However, the same economies of scale may increase dependence on a small number of suppliers.

This dependence can create a single point of failure. If a widely used model, cloud service, or computing platform experiences a major outage, cyberattack, or operational failure, the consequences may extend to numerous organizations that rely on it. Firms may also encounter high switching costs if their applications depend on provider-specific interfaces, data formats, or proprietary tools.

The FSB (2024) identifies third-party dependencies and concentration among the important AI-related vulnerabilities relevant to financial stability. Similar mechanisms may affect other critical sectors that depend on digital infrastructure.

Infrastructure dependence also has a geopolitical dimension. Advanced semiconductors, data-center capacity, and reliable energy supplies have become strategically significant resources. Restrictions on access to these resources may influence national technological capabilities and create vulnerabilities in international supply chains.

The principal finding in this domain is that AI-related economic security cannot be assessed solely at the level of individual models. It also depends on the structure of the markets and infrastructure through which AI is developed, distributed, and maintained.

Financial-System Vulnerabilities

Financial institutions use AI in activities such as fraud detection, credit assessment, customer service, risk analysis, and trading. These applications can improve efficiency and help institutions process large volumes of information. However, their growing adoption also creates new forms of operational and systemic exposure.

International Scientific Journal of Contemporary Research in Social Sciences and Humanities
2026 / No. 1 (1)
ELECTRONIC JOURNAL | OPEN ACCESS
Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

The FSB (2024) identifies several relevant vulnerabilities, including third-party dependencies, market correlations, cyber risk, and model risk. These vulnerabilities can interact.

One concern is correlated decision-making. If many institutions rely on similar models, training data, or optimization objectives, their responses to new information may become more alike. During periods of stress, this similarity could reinforce common trading decisions, reduce market diversity, or contribute to procyclical behavior. The precise magnitude of these effects remains uncertain and requires empirical investigation.

A second concern is model opacity. Complex systems may be difficult to interpret, making it challenging for institutions and supervisors to determine why a model generated a particular output or whether its performance will remain reliable under unusual conditions. Models that perform well in normal circumstances may behave differently when market conditions change sharply.

Third-party dependence creates an additional operational risk. If a financial institution relies on an external AI provider, disruption at that provider may affect multiple services simultaneously. The resulting effects may be difficult to anticipate when institutions assess vendor relationships separately.

These findings suggest that AI-related financial vulnerabilities extend beyond the accuracy of individual models. They involve common exposures, interconnected service providers, and the possibility that failures could occur simultaneously across institutions.

Malicious Use and Geoeconomic Competition

AI can also reduce the resources required to produce certain forms of deception and digital attack. Brundage et al. (2018) examined how AI might facilitate malicious activities, including cyberattacks, social engineering, and disinformation. Subsequent safety assessments have continued to examine the implications of AI-enabled fraud, scams, and cyber operations, while recognizing that evidence about the scale and effectiveness of some capabilities remains incomplete (Bengio et al., 2025).

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Generative systems can produce convincing text, images, audio, and other digital material. These capabilities may help malicious actors personalize fraudulent messages, impersonate trusted individuals, or generate misleading content at scale. The resulting economic consequences may include direct financial losses, higher verification costs, and reduced confidence in digital transactions.

The broader concern is the reliability of information. Markets depend on the ability of participants to verify identities, assess information, and trust transaction processes. As synthetic content becomes more accessible, institutions may need stronger authentication and verification mechanisms.

At the state level, AI is increasingly connected to strategic competition. Governments have incentives to secure access to advanced chips, computing capacity, data, talent, and energy. Export controls and other restrictions may be used to protect national security interests, but they can also fragment supply chains and complicate international cooperation.

The review identifies malicious use and geopolitical competition as related but distinct challenges. The first concerns the exploitation of AI capabilities by harmful actors; the second concerns strategic decisions by states that influence access to technology and the resilience of international economic networks.

Governance Gaps and Institutional Constraints

The reviewed governance frameworks address important aspects of AI risk, but their scope, legal status, and enforcement mechanisms differ.

The OECD AI Principles, adopted in 2019 and updated in 2024, provide an intergovernmental framework for responsible AI development and use. The European Union AI Act establishes a legally binding, risk-based regulatory framework with obligations that vary according to the relevant system and activity (European Parliament & Council of the European Union, 2024). In the United States, the NIST AI Risk Management Framework offers guidance for identifying, assessing, and managing AI-related risks (National Institute of Standards and Technology, 2023).

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

These approaches provide useful foundations, but they do not create a fully coordinated international system for managing AI-related economic security. Differences in regulatory requirements may increase compliance costs for firms operating across borders. Differences in institutional capacity may also produce uneven levels of protection.

A further problem is the distribution of responsibilities. Labor ministries may focus on employment transitions, competition authorities on market structure, financial supervisors on institutional stability, and cybersecurity agencies on digital threats. Yet AI-related shocks can affect all these areas simultaneously.

Evidence and timing create additional difficulties. The International AI Safety Report discusses the challenge of deciding when to intervene in the presence of uncertainty (Bengio et al., 2025). Early regulation may impose unnecessary costs or become outdated, whereas delayed intervention may allow vulnerabilities to become deeply embedded in critical systems.

Effective governance also requires technical expertise, reliable incident reporting, and access to relevant information. Public institutions that lack these resources may struggle to evaluate claims made by technology providers or assess the consequences of complex systems.

Taken together, the literature points to a governance gap characterized by fragmented responsibilities, uneven enforcement capacity, incomplete evidence, and limited coordination across jurisdictions.

Summary of Findings

The findings can be summarized by connecting each risk domain to its principal vulnerability and a corresponding resilience response.

Risk domain	Principal vulnerability	Governance challenge	Resilience response
Labor markets	Displacement and unequal	Insufficient transition support	Retraining, wage insurance,

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

	distribution of gains		employment services
Market concentration	Dependence on a limited number of providers	Difficulties addressing AI supply-chain power	Interoperability, competition policy, alternative providers
Financial stability	Correlated models and shared service dependencies	Incomplete monitoring and stress testing	Dependency mapping, model validation, AI-aware stress tests
Malicious use	Fraud, impersonation, and cyber operations	Cross-border enforcement difficulties	Incident sharing, authentication, coordinated security measures
Geoeconomic competition	Concentrated access to strategic resources	Fragmented international approaches	Supply-chain resilience and international coordination

Note. The table synthesizes the themes identified in the literature reviewed in this article.

Discussion.

From Individual Risk Management to Systemic Resilience

The findings indicate that AI-related economic security is a systemic problem rather than a collection of independent technical concerns. Labor-market disruption affects household income and demand. Infrastructure concentration creates shared operational vulnerabilities. Financial institutions may respond similarly to shocks when they depend on comparable models. Malicious use can weaken trust in digital transactions, while geopolitical competition can disrupt access to essential resources.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

These mechanisms suggest that policies focused exclusively on individual model accuracy or organizational compliance may be insufficient. A model can perform well in isolation while still contributing to a broader vulnerability if it is deployed widely, depends on a single provider, or encourages similar decisions across institutions.

Resilience provides a useful framework for addressing these interconnected risks. Rather than assuming that every failure can be prevented, resilience focuses on reducing exposure, maintaining essential functions during disruption, recovering efficiently, and adapting to new conditions. This approach is especially relevant when technological capabilities and economic consequences are changing faster than the evidence can fully establish their long-term effects.

Adaptive and Risk-Proportionate Regulation

Regulation should be proportionate to the potential consequences of an AI application. Systems that influence access to essential services or support high-impact financial decisions may warrant more extensive safeguards than applications used for low-stakes administrative tasks.

The risk-based approach reflected in the EU AI Act offers one reference point, while the NIST AI Risk Management Framework provides practical guidance for managing risks throughout the AI life cycle. However, the effectiveness of these approaches depends on implementation, institutional capacity, and the availability of evidence.

Regulators should combine established rules with mechanisms for learning. Regulatory sandboxes can help authorities and firms evaluate new applications under controlled conditions. Incident-reporting requirements can reveal recurring failures, while scheduled reviews can allow requirements to evolve as evidence changes.

Adaptive regulation should not mean indefinite delay. Where credible evidence indicates a risk of severe or widespread harm, safeguards may be justified even when the probability and magnitude of future damage cannot be estimated precisely. At the same time, regulatory requirements should be reviewed to avoid unnecessary burdens that prevent beneficial innovation.

International Scientific Journal of Contemporary Research in Social Sciences and Humanities
2026 / No. 1 (1)
ELECTRONIC JOURNAL | OPEN ACCESS
Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Competition Policy and Infrastructure Resilience

Market concentration creates a policy challenge because the same economies of scale that support AI development may also create dependence. Competition authorities should therefore consider the structure of the wider AI supply chain, including cloud computing, semiconductor access, model distribution, and the services needed to integrate AI into business operations.

Interoperability and data portability may reduce switching costs when technically and legally appropriate. Publicly supported computing resources can also widen access to research infrastructure and reduce barriers for universities, small firms, and public-interest projects.

Organizations operating critical services should avoid treating a single provider as an unavoidable dependency. Multi-provider strategies, backup arrangements, tested exit plans, and contingency procedures can help maintain essential functions during an outage. These measures should be evaluated according to the criticality of the service and the feasibility of switching, since maintaining multiple providers may itself introduce additional costs and complexity.

The broader objective is not to eliminate large technology providers but to ensure that their failure, withdrawal, or loss of availability does not automatically become a widespread economic disruption.

Financial Supervision and System-Wide Stress Testing

Financial supervisors should assess AI adoption as part of operational resilience and systemic-risk monitoring. Institutions can begin by identifying where AI is used in important functions, which external providers support those functions, and how disruptions might affect customers, counterparties, and other institutions.

Model validation should examine not only average performance but also behavior under unusual conditions. Supervisors and institutions should consider whether models remain reliable when market conditions shift, whether their decisions are excessively correlated, and whether alternative processes are available if a model becomes unavailable.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Stress testing can incorporate hypothetical scenarios involving the simultaneous failure of a widely used model or cloud provider, a large-scale AI-enabled fraud campaign, or a period in which similar automated strategies amplify market volatility. Such exercises would not predict future events precisely; their purpose would be to identify weaknesses and test contingency plans.

Human oversight should be meaningful rather than merely procedural. Staff responsible for high-impact decisions need sufficient expertise, authority, and access to information to question automated outputs and intervene when appropriate.

These measures would help supervisors assess AI-related risks as potential sources of interconnected failure rather than treating every deployment as an isolated technology project.

Workforce Investment and Social Protection

Labor-market resilience requires policies that help workers move into new activities while maintaining economic security during the transition. The objective should not be to preserve every existing task or occupation indefinitely, but to ensure that technological gains do not impose disproportionate costs on workers who have limited resources to adjust.

Active labor-market policies can include targeted retraining, employment services, career guidance, and support for mobility. Training programs should be linked to credible labor-market demand rather than designed around the assumption that every worker can transition into a technical occupation.

Wage insurance or temporary income support may help workers whose earnings fall after displacement. Portable training entitlements can allow workers to obtain new skills throughout their careers, while employer-supported development can help employees adapt before their roles become obsolete.

Tax and subsidy arrangements should also be assessed for unintended incentives that favor replacing workers over improving their productivity. Acemoglu and Restrepo (2019) emphasize the importance of new task creation in shaping the labor-market

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

effects of automation. Policies that support innovation complementary to human work may therefore contribute to a more inclusive transition.

International differences matter as well. The IMF finds that economies differ in their exposure and preparedness for AI (Cazzaniga et al., 2024). Countries with limited digital infrastructure, financial resources, or training capacity may struggle to capture benefits while absorbing adjustment costs. International assistance should consequently include education, institutional capacity, and access to appropriate infrastructure.

International Coordination and Shared Evidence

AI supply chains and digital services operate across national borders, making purely domestic solutions incomplete. A major provider may serve customers in many jurisdictions, while cyber operations and financial consequences can spread internationally.

International cooperation should prioritize compatible incident-reporting practices, information exchange, and shared methods for evaluating high-impact AI systems. Common approaches can help authorities identify emerging threats while reducing unnecessary duplication across jurisdictions.

Cooperation should also extend to technical expertise and capacity-building. Lower-income countries need opportunities to participate in decisions about standards, access to infrastructure, and the distribution of economic benefits. Otherwise, international governance may reflect the priorities of countries and firms with the greatest resources while leaving other economies more exposed to external decisions.

Coordination does not require every country to adopt identical rules. Different legal systems and economic conditions may justify different implementation choices. The practical goal is to improve the compatibility of safeguards, increase the availability of reliable evidence, and reduce the likelihood that regulatory gaps become channels through which systemic risks spread.

An Integrated Resilience Framework

The policy implications can be organized into five mutually reinforcing pillars.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

First, adaptive governance should establish proportionate safeguards, incident reporting, regular review, and clear institutional responsibilities.

Second, infrastructure resilience should reduce excessive dependence on individual providers through competition policy, interoperability, backup arrangements, and realistic exit plans.

Third, financial resilience should incorporate AI dependencies into supervisory monitoring, model validation, operational continuity planning, and system-wide stress testing.

Fourth, social resilience should support workers through training, employment services, income protection, and policies that encourage productive uses of AI.

Fifth, international resilience should strengthen shared evidence, compatible standards, cross-border incident response, and participation by countries with different levels of technological capacity.

The pillars are interdependent. For example, infrastructure diversification may be ineffective if smaller providers lack adequate security, while workforce training may have limited value if the jobs created by technological change are geographically inaccessible. Similarly, incident reporting cannot improve governance if institutions lack the resources to analyze the information collected.

Implementation should therefore be guided by measurable outcomes. Governments can monitor worker transitions and wage changes, the concentration of critical services, the frequency and severity of AI-related incidents, and the effectiveness of institutional recovery plans. Such monitoring would allow policies to be adjusted as evidence accumulates.

Limitations and Future Research

This article has several limitations. First, it relies on a selected narrative synthesis rather than an exhaustive systematic review. Relevant research may therefore have been omitted. Second, many estimates of AI's future effects are based on task exposure, scenarios, or projections rather than observed long-term outcomes. Exposure does not translate directly into job losses, productivity gains, or financial instability.

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

Third, the pace of technological change means that some assessments may become outdated as capabilities, business models, and regulations evolve. Fourth, the article proposes an integrated policy framework but does not empirically test the effectiveness or cost of each intervention.

Future research should examine realized labor-market outcomes across occupations and countries, the relationship between AI adoption and market concentration, and the conditions under which shared models increase systemic risk. Comparative studies could also assess which regulatory approaches improve safety without unnecessarily restricting beneficial innovation. Finally, further research is needed to determine how public institutions can measure AI-related economic security using reliable indicators and comparable cross-country data.

Conclusion.

Artificial intelligence has the potential to improve productivity, expand access to analytical capabilities, and strengthen the detection of fraud and other threats. At the same time, it can create vulnerabilities that affect employment, market structure, financial stability, and confidence in digital transactions. These risks are not determined by technology alone; they depend on how AI is deployed, who controls essential infrastructure, how economic gains are distributed, and whether institutions can respond effectively to disruption.

The literature reviewed in this article identifies four principal risk domains: labor-market disruption, concentration and infrastructure dependence, financial-system fragility, and malicious or geopolitical misuse. Across these domains, several common problems emerge. Economic benefits and adjustment costs may be distributed unevenly, critical services may depend on a limited number of providers, similar models may create correlated behavior, and governance institutions may lack sufficient evidence or technical capacity.

A resilient approach requires coordinated action across regulation, competition policy, financial supervision, workforce development, and international cooperation. Governments should adopt proportionate safeguards and improve their capacity to learn

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

from incidents. Firms should map dependencies, validate important models, and prepare credible continuity plans. Labor-market institutions should help workers adapt while protecting them against severe income shocks. International bodies should promote shared evidence and compatible standards while ensuring that lower-income economies can participate meaningfully in governance.

The central conclusion is that economic security in the age of AI should be understood as the ability to benefit from technological progress without allowing its risks to become uncontrollable sources of social or systemic instability. Prevention remains important, but resilience is equally essential because uncertainty cannot be eliminated. Building institutional capacity, reliable data, diversified infrastructure, and mechanisms for cooperation now may reduce the economic and social costs of future disruptions.

References:

1. Acemoglu, D. (2024). The simple macroeconomics of AI (NBER Working Paper No. 32487). National Bureau of Economic Research. https://doi.org/10.3386/w32487
2. Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. Journal of Economic Perspectives, 33(2), 3–30. https://doi.org/10.1257/jep.33.2.3
3. Autor, D. H. (2015). Why are there still so many jobs? The history and future of workplace automation. Journal of Economic Perspectives, 29(3), 3–30. https://doi.org/10.1257/jep.29.3.3
4. Bengio, Y., Mindermann, S., Privitera, D., et al. (2025). International AI safety report (arXiv:2501.17805). https://arxiv.org/abs/2501.17805
5. Bommasani, R., Hudson, D. A., Adeli, E., et al. (2021). On the opportunities and risks of foundation models (arXiv:2108.07258). https://arxiv.org/abs/2108.07258

Received: 10 October 2026, Accepted: 20 October 2026, Published: 22 October 2026

6. Brundage, M., Avin, S., Clark, J., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation (arXiv:1802.07228). https://arxiv.org/abs/1802.07228
7. Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton.
8. Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A. J., Pizzinelli, C., Rockall, E., & Tavares, M. M. (2024). Gen-AI: Artificial intelligence and the future of work (IMF Staff Discussion Note SDN/2024/001). International Monetary Fund.
9. Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2024). GPTs are GPTs: Labor market impact potential of LLMs. Science, 384(6702), 1306–1308. https://doi.org/10.1126/science.adj0998
10. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689.
11. Financial Stability Board. (2024). The financial stability implications of artificial intelligence. https://www.fsb.org
12. Korinek, A., & Stiglitz, J. E. (2019). Artificial intelligence and its implications for income distribution and unemployment. In A. Agrawal, J. Gans, & A. Goldfarb (Eds.), The economics of artificial intelligence: An agenda (pp. 349–390). University of Chicago Press.
13. National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
14. Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on artificial intelligence (OECD/LEGAL/0449; amended 2024). https://legalinstruments.oecd.org