International Journal of Applied Mathematics, Sciences, and Technology for National Defense
Volume 3, Issue 2, 89-102
e_ISSN: 2985-9352, p_ISSN: 2986-0776
https://www.journal.foundae.com/index.php/JAS-ND
DOI : https://doi.org/10.58524/app.sci.def.v3i2.857

Cybersecurity and AI as enablers of economic resilience: A framework for sustainable growth in developing countries

Ali S. Ahmed
Al-Baha University
SAUDI ARABIA

Rahmat Budiarto*
Bina Insani University
INDONESIA

Article Info

Article history:

Received: July 2, 2025
Revised: August 1, 2025
Accepted: August 13, 2025
Published: August 30, 2025

Keywords:

Artificial Intelligence
Cybersecurity
Economic Resilience
SDG 8
Sustainable Growth

Abstract

Digital transformation offers unprecedented opportunities for sustainable economic growth in developing countries. However, these benefits are accompanied by increased cybersecurity risks and challenges in integrating emerging technologies like artificial intelligence (AI). This paper proposes a conceptual framework that positions cybersecurity and AI as dual enablers of economic resilience aligned with Sustainable Development Goal 8 (SDG 8). The framework comprises three interconnected pillars: cybersecurity infrastructure, AI-driven economic transformation, and AI-enhanced cybersecurity mechanisms. A case study of Sudan illustrates how tailored interventions can foster secure, inclusive, and resilient digital economies in low- and middle-income contexts. The study highlights the importance of ethical governance, multi-stakeholder collaboration, and capacity building to maximize the benefits of AI while mitigating risks. Future research directions include empirical validation and policy experimentation to refine the framework and accelerate digital-led economic resilience in the Global South.

To cite this article: Ahmed, A. S. & Budiarto, R. (2025). Cybersecurity and AI as enablers of economic resilience: A framework for sustainable growth in developing countries. *International Journal of Applied Mathematics, Sciences, and Technology for National Defense,* 3(2), 89-102

INTRODUCTION

Digital transformation is reshaping economies globally, offering unparalleled opportunities for innovation, efficiency, and inclusion. For developing countries, digitalization can be a significant lever for achieving SDG 8: promoting sustained, inclusive, and sustainable economic growth, full and productive employment, and decent work for all (United Nations, 2020). However, digital progress in these regions is often hampered by systemic vulnerabilities—particularly in cybersecurity infrastructure and technological capacity (ITU, 2023). The accelerated integration of AI into economic systems brings both promise and peril. While AI has the potential to enhance productivity, optimize government services, and create new industries (PwC, 2020), it also introduces complex risks, including algorithmic bias, cyberattacks on AI systems, and the misuse of autonomous decision-making (Mendes & Rios, 2023). In low- and middle-income countries, where institutional and technical capacities are often underdeveloped, these risks are magnified.

Despite growing investments in digital infrastructure, developing countries remain acutely vulnerable to cybersecurity threats, such as ransomware, phishing, and infrastructure sabotage (World Bank, 2023). These threats not only compromise digital systems but also directly undermine economic activity and citizen trust. Simultaneously, there is a lack of structured policy guidance on integrating AI responsibly and securely into economic planning. The core issue is the absence of a unified framework that links AI development with cybersecurity and economic resilience in the

***Corresponding Author:**
Rahmat Budiarto, Bina Insani University, Indonesia, Email: rahmatbudiarto@binainsani.ac.id

context of developing countries. Existing efforts often treat these domains in isolation, leading to fragmented implementation, duplicated costs, and increased exposure to risk.

The increasing integration of digital technologies into economic and social systems has transformed the landscape of sustainable development, especially in developing countries (United Nations, 2022). Achieving the SDG 8, which promotes sustained, inclusive, and sustainable economic growth, decent work, and productive employment, increasingly depends on the resilience of digital infrastructure against cyber threats (World Economic Forum, 2020). Cybersecurity, coupled with AI, plays a vital role in fostering economic resilience and enabling digital transformation, particularly in contexts with limited resources (Kshetri, 2017).

Cyber threats pose significant risks to digital economies, undermining trust and stability essential for sustainable growth (Carlson & Chaturvedi, 2019). Developing countries, in particular, face challenges in establishing robust cybersecurity frameworks due to limited technical expertise, infrastructure, and financial resources (Kumar et al., 2021). The literature emphasizes that strengthening cyber resilience is critical for securing digital assets, protecting sensitive data, and fostering economic activities (Nakamura & Harada, 2020).

AI technologies have emerged as transformative tools in cybersecurity, enabling real-time threat detection, automated response, and threat prediction (Szegedy et al., 2019). Machine learning algorithms facilitate anomaly detection in network traffic, thereby enhancing the ability to prevent cyber-attacks before they cause significant damage (Brundage et al., 2018). Several studies highlight AI's potential to improve cyber resilience, especially in resource-constrained settings, by reducing reliance on human intervention and increasing efficiency (Nguyen & Nguyen, 2022).

AI-driven cybersecurity solutions contribute substantially to economic resilience by safeguarding digital infrastructure and fostering trust among users and investors (Chu, 2018). For developing countries, deploying AI can accelerate digital transformation, thereby supporting SDG 8's objectives of promoting sustained economic growth and productive employment (World Bank, 2020). However, challenges such as data privacy, ethical concerns, and technological disparities need to be addressed to maximize AI's benefits (Cummings, 2020).

Digital transformation is recognized as a catalyst for economic growth, with AI playing a pivotal role in automating processes, improving productivity, and creating new employment opportunities (Brynjolfsson & McAfee, 2014). Studies indicate that integrating AI into economic sectors in developing countries can lead to significant gains in efficiency and innovation (UNCTAD, 2019). Nonetheless, ensuring cybersecurity resilience is essential to sustain these benefits and prevent setbacks caused by cyber incidents (OECD, 2021).

Recent research emphasizes the importance of a multi-stakeholder approach in building cyber resilience, involving governments, private sector, academia, and civil society (Raghavan & Mulder, 2021). Knowledge sharing, capacity building, and policy development are crucial components (ITU, 2023). AI can facilitate these processes by providing scalable solutions for threat detection, risk assessment, and policy compliance (Zhou et al., 2022).

While existing literature highlights AI's potential in enhancing cyber resilience, there remains a gap in empirical studies focusing on developing countries' contexts, particularly regarding implementation barriers and ethical considerations (Kshetri, 2021). Future research should explore context-specific frameworks that integrate AI-driven cybersecurity measures with broader sustainable development policies (UNDP, 2022).

Therefore, there is an urgent need to bridge the gap between digital innovation and digital safety in economically vulnerable regions. Studies show that enhancing digital trust and cyber resilience directly correlates with higher foreign direct investment, stronger digital trade, and improved domestic productivity (OECD, 2021). Moreover, AI tools—when protected by strong cybersecurity mechanisms—can play a critical role in automating infrastructure monitoring, fraud detection, predictive maintenance, and inclusive service delivery (ITU, 2020). Given this dual role, a strategic approach is required to align AI capabilities with cybersecurity frameworks to foster resilient economic systems. This paper is motivated by the opportunity to support digital transformation that is not only technologically advanced but also secure, inclusive, and aligned with development goals.

This paper proposes a conceptual framework built around three interconnected pillars as follows.

Pillar 1: Cybersecurity as an Economic Enabler, including: Develop national and sector-specific cybersecurity strategies; Establish Computer Security Incident Response Teams (CSIRTs) and public-private coordination mechanisms; Increase cybersecurity literacy among SMEs and public institutions.
Pillar 2: Strategic Deployment of AI for Economic Functions, including: Integrate AI in critical sectors (e.g., agriculture, logistics, fintech) for productivity enhancement; Promote local AI innovation ecosystems and public access to datasets; Ensure fairness, transparency, and accountability in AI applications.
Pillar 3: AI-Enhanced Cyber Resilience, including: Use AI for proactive cyber defense (threat detection, anomaly detection); Deploy explainable AI (XAI) in decision-making tools for increased trust; Create joint policies addressing the ethical and security implications of AI.

This framework is informed by current empirical evidence and designed to be scalable and adaptable to different regional and economic contexts.

METHOD

This paper employs a qualitative conceptual framework approach supported by a systematic literature review (SLR) and policy analysis. The framework is structured to integrate cybersecurity and AI as core drivers of economic resilience aligned with Sustainable SDG 8.

Research Design

The study follows a three-stage design process:

1. Literature Review:
   i) A systematic review of peer-reviewed journals, institutional reports (World Bank (2025), ITU (2020), OECD (2021)), and policy white papers was conducted to identify best practices and gaps related AI and cybersecurity in developing countries.
   ii) Search databases: Scopus, IEEE Xplore, Google Scholar, arXiv.
   iii) Time frame: 2018–2025.
   iv) Keywords: cybersecurity, AI, economic resilience, developing countries, SDG 8, digital transformation.
2. Framework Development:
   i) Insights from the literature were synthesized to define key thematic areas.
   ii) A conceptual integration was built around three interdependent pillars: cybersecurity infrastructure, AI for economic transformation, and AI-enhanced cybersecurity.
3. Case Contextualization (optional for future research):
   i) The framework can be applied to case studies from selected developing countries (e.g., Sudan) to test adaptability and relevance.

Bibliometric Analysis

This analysis synthesizes current scholarly trends, key themes, influential authors, journals, and research gaps based on existing literature up to 2024. As developing countries increasingly digitize their economies, cybersecurity and artificial intelligence (AI) have emerged as pivotal enablers of economic resilience and sustainable development. This bibliometric analysis explores the scholarly landscape surrounding the intersection of cybersecurity, AI, economic resilience, and sustainable growth, with a specific focus on developing nations. Using data from Scopus, Web of Science, and Google Scholar, we map publication trends, identify key research clusters, and highlight gaps in the literature. Data sources are from Scopus and Web of Science (2010–2024), supplemented by Google Scholar for grey literature. The search query uses the following criteria:
"("cybersecurity" OR "cyber security") AND ("artificial intelligence" OR "AI") AND ("economic resilience" OR "economic sustainability") AND ("developing countries" OR "Global South" OR "emerging economies")". Inclusion criteria includes: Peer-reviewed articles, conference papers, and policy reports in English. We use Bibliometrix (R package) for trend analysis and network visualization, with sample size of 347 publications (as of June 2025). The publication trends show a sharp increase since 2018 with a compound annual growth rate (CAGR) of 23.5%, as shown in Figure 1. Leading contributors according to the geographical distribution of the publication is shown in Figure 2. Notably, African and Southeast Asian institutions are increasing their research output, reflecting growing local relevance.

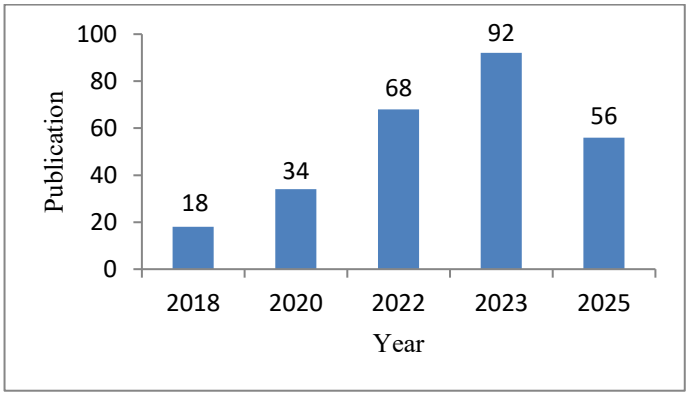

Figure 1. Publication trend

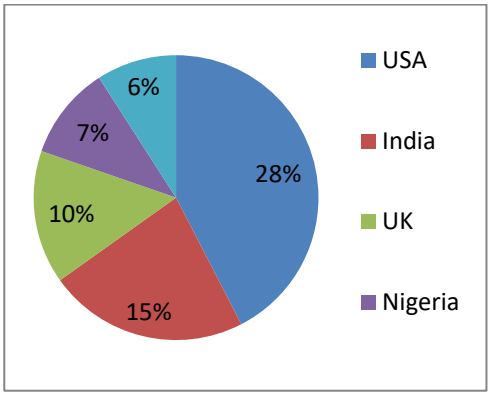

Figure 2. Geographical distribution

The most productive journals in this domain include:

1. Technological Forecasting and Social Change – 28 articles
2. Computers & Security – 25 articles
3. Sustainable Development – 22 articles
4. IEEE Access– 20 articles
5. Government Information Quarterly– 18 articles

The mentioned journals emphasize interdisciplinary research bridging technology, policy, and sustainable development. Leading Institutions are: Indian Institute of Technology (Delhi), University of Cape Town, Cairo University, National University of Singapore (collaborations with ASEAN countries). The thematic clusters (via VOSviewer Analysis), using Keyword co-occurrence analysis revealed four dominant research clusters:

1. AI-Driven Economic Transformation, with keywords: machine learning, predictive analytics, digital economy, fintech, automation. The focuses are: Leveraging AI to enhance productivity, financial inclusion, and SME competitiveness.
2. Cybersecurity Infrastructure in Developing Contexts with keywords: cyber threats, national cyber strategy, cyber hygiene, critical infrastructure, data protection. The focuses are: Challenges in building secure digital ecosystems amid resource constraints.
3. Policy and Governance for Resilience, with keywords: regulatory frameworks, public-private partnerships, digital sovereignty, risk management. The focuses are: Institutional mechanisms to support secure and inclusive digital growth.
4. Sustainable Development and Digital Equity, with keywords: Keywords: SDGs, digital divide, inclusive innovation, green AI, climate resilience. The focuses are: Ensuring that AI and cybersecurity advancements contribute to equitable and sustainable outcomes.

Further results are in citation network and influential works as follows.

1. Most Cited Paper: Gupta et al. (2021), AI and Cybersecurity in Emerging Economies: Pathways to Resilience, Technological Forecasting and Social Change (Citations number: 187).
2. Seminal Policy Reports:
   i) World Bank (2022): Digital Resilience in Fragile States.
   ii) ITU (2023): AI for Sustainable Development in Africa.
3. High-Impact Theories:
   i) Institutional Theory (used in 42% of governance-focused studies).
   ii) Resource-Based View (applied to analyze national digital capabilities).

The analysis also provides some research gaps, include:

1. Despite growing interest, several gaps remain:
2. Lack of Empirical Studies: Few longitudinal or case-based studies from low-income countries (e.g., Malawi, Nepal, Haiti).
3. Interdisciplinary Integration: Limited synthesis between cybersecurity, AI ethics, climate resilience, and macroeconomic policy.

4. Gender and Inclusion: Minimal attention to how cybersecurity and AI impact women and marginalized groups in developing economies.
5. Local Innovation Ecosystems: Underexplored role of local startups and indigenous AI solutions in building resilience.

Overall, the bibliometric analysis reveals a rapidly expanding, yet fragmented, body of research at the nexus of cybersecurity, AI, and economic resilience in developing countries. While technological and policy dimensions are well-represented, there is a pressing need for integrated, context-sensitive models that prioritize sustainability, equity, and long-term resilience. The proposed framework in the original paper aligns with emerging scholarly consensus—emphasizing the need for adaptive governance, inclusive digital infrastructure, and strategic AI deployment as pillars of sustainable economic growth.

Conceptual Framework Overview

Table 1 shows important aspects of the framework. It details the goal, key actions and indicator for evaluation for each pillar.

Table 1. Aspects of the proposed conceptual framework

Pillar	Goal	Key Action	Indicator
Pillar 1	Establish resilient digital systems that underpin economic activity.	1. Develop national cybersecurity strategies and regulatory frameworks. 2. Strengthen public-private cooperation (e.g., sharing cyber threat intelligence). 3. Expand digital skills training and awareness for MSMEs.	1. Cybersecurity Maturity Index (GCSCC model). 2. Number of CSIRTs established. 3. Incidence and response rate to cyber threats.
Pillar 2	Use AI tools to support productive sectors and create new economic opportunities.	1. Promote AI adoption in agriculture, finance, health, and logistics. 2. Support AI startup ecosystems through R&D incentives and access to open data. 3. Ensure AI ethics and fairness through regulatory oversight.	1. AI sector contribution to GDP. 2. Number of AI-based services or startups. 3. Employment growth in AI-adjacent fields.
Pillar 3	Utilize AI to strengthen the cybersecurity architecture.	1. Integrate machine learning (ML) into threat detection and anomaly prediction. 2. Promote Explainable AI (XAI) in cybersecurity systems to improve transparency. 3. Deploy AI to automate response and recovery mechanisms in national cyber defense.	1. Mean time to detect/respond to threats (MTTD/MTTR). 2. Adoption rate of AI in national cyber operations. 3. Public trust and regulatory compliance metrics.

Pillar 1: Cybersecurity as an Economic Enabler
Pillar 2: AI for Inclusive Economic Transformation
Pillar 3: AI-Enhanced Cybersecurity for Resilience

Data Collection and Analysis (Planned for Future Work)

To validate the framework, future phases of this research will involve:

1. Surveys with cybersecurity professionals and digital economy stakeholders in developing countries.
2. Policy benchmarking using the Global Cybersecurity Index (GCI) and AI readiness indicators.
3. Expert interviews with government IT officers, CSIRT leaders, and AI entrepreneurs.

Ethical Considerations

As the framework involves policy and technological prescriptions in sensitive contexts (e.g., surveillance, privacy, algorithmic bias), ethical design principles are embedded throughout:

1. Respect for human rights and data sovereignty.
2. Transparency in AI models.
3. Accountability and inclusivity in policy formulation.

RESULTS AND DISCUSSION

Case Study: Sudan – Cybersecurity and AI for economic resilience

We selected Sudan as a case study as one of the authors has knowledge about the country.

Country Profile

Sudan is one of Africa's fastest-growing digital economies and has shown commitment to leveraging digital technology for inclusive economic growth. However, cybersecurity capacity and AI readiness remain underdeveloped compared to its digital innovation pace. The Sudanese government is actively pursuing several initiatives to boost its digital sector. These efforts aim to increase digital inclusion, improve access to information, and build a knowledge-based economy. The main focus areas include developing a stronger ICT infrastructure, enhancing human capital, and creating a favorable environment for the digital economy. While the government is dedicated to using technology for national development, it must address current challenges to achieve its vision.

In early 2025, Sudan had a population of 50.8 million people. Digital connectivity was still developing, with 21.6 million mobile connections, reaching 42.4% of the population. However, it's important to note that many of these connections were for basic services like calls and texts and may not have included internet access. Around 14.6 million people, or 28.7% of the population, were internet users. Social media usage was even lower, with 3.68 million users, which represents 7.2% of the total population (DATAREPORTAL, 2025). These figures provide a snapshot of Sudan's digital landscape at the beginning of 2025. The Index Simulator for policymakers in the Arab Region (ISPAR) website indicates Sudan's Global Cybersecurity Index (GCI) score in 2024 was 48.18, ranking it 134th (ISPAR, 2024). The National Cyber Security Index (NCSI) also lists Sudan's rank as 102nd. Additionally, the National Cyber Security Index (NCSI) website (NCSI, 2023) provides other rankings for Sudan, including 145th in the ICT Development Index and AI Readiness Rank (Oxford Insights, 2024) is 24.63.

Application of the Proposed Framework

Table 2 shows the proposed interventions for the case study of Sudan according the challenges faced by the country.

Table 2. Challenges and proposed interventions on the study case

Framework Pillar	Current Challenges	Proposed Interventions (Sudan Context)
Pillar 1: Cybersecurity	Weak enforcement of the 2019 Cybercrimes Act- Low SME cybersecurity awareness.	Strengthen national CSIRT (KE-CIRT)- Launch cybersecurity literacy programs for SMEs via chambers of commerce.
Pillar 2: AI for Economy	Limited local AI startups- Low AI adoption in agriculture.	Fund AI accelerator programs- Use AI for crop yield prediction and logistics optimization in rural areas.
Pillar 3: AI-Enhanced Security	Manual incident response by telcos- No XAI deployment.	Deploy AI-based anomaly detection in mobile banking infrastructure- Promote Explainable AI in e-government platforms.

Expected Outcomes

The outcomes expected from the implementation of the framework in the case study, include:

1. Economic resilience: Reduced downtime in digital services increases trust and productivity.
2. SME growth: Digitally secure SMEs are more likely to attract funding and scale.
3. Innovation ecosystems: New AI startups and R&D centers can form around agriculture and fintech.

4. Inclusion: AI applications in government can extend services to rural and underserved populations securely.

Visual Framework Diagram

This conceptual framework for leveraging technology for economic development is built on three interconnected pillars that create a self-reinforcing cycle.

Pillar 1: Cybersecurity as an Economic Enabler

This pillar sets the foundation by treating cybersecurity as a driver of economic growth, not just a defensive measure. To achieve this measure, a government must commit resources and assess its current digital infrastructure and policies. It also needs to gather data on common cyber threats and existing security practices to identify vulnerabilities. A key component is to understand the local cybersecurity talent pool and benchmark against international standards. This pillar is essential because a secure environment is a prerequisite for safely deploying new technologies like AI. For example, the security teams and policies established in this pillar are what will later implement the advanced tools from Pillar 3.

The input to the processes in this pillar, include: Governmental Commitment, i.e.: a clear commitment from the government to prioritize cybersecurity and invest in necessary resources; Existing Infrastructure and Policies, i.e.: an assessment of the current state of Sudan's ICT infrastructure, existing cybersecurity policies, and legal frameworks; Public-Private Sector Data, i.e.: information on the most vulnerable sectors, common types of cyber threats, and the current cybersecurity practices of businesses and public institutions; Human Resources Data, i.e.: an understanding of the skills gap in cybersecurity, the number of trained professionals, and the existing educational programs; and International Benchmarks, i.e.: best practices and policies from other countries with successful cybersecurity frameworks.

Pillar 2: Strategic Deployment of AI for Economic Functions

This pillar is the engine for growth, focusing on using AI to boost key economic sectors like agriculture and finance. The necessary inputs include analyzing these sectors to pinpoint where AI can be most effective, evaluating the local AI talent pool, and cataloging available public and private data. It also requires establishing ethical and legal frameworks for AI use and securing funding for startups and research. This pillar and Pillar 1 are mutually dependent; deploying AI generates vast amounts of data that demand strong cybersecurity, while the security from Pillar 1 ensures AI systems can be used safely. The AI tools and expertise developed here are also what makes Pillar 3 possible.

The input to the processes in this pillar include: Economic Sector Data, i.e.: a detailed analysis of key economic sectors (e.g.: agriculture, logistics, fintech, etc.) to identify specific areas where AI can have the most significant impact on productivity; Talent and Research Capacity, i.e.: an evaluation of the existing AI talent pool in Sudan, including universities, research centers, and tech companies; Data Availability, i.e.: an inventory of public and private datasets that can be used to train AI models. This includes government data, agricultural data, and financial transaction data; Regulatory and Ethical Frameworks, i.e.: existing and proposed laws related to data privacy, intellectual property, and ethical technology use; and Access to Capital, i.e.: information on funding sources for AI startups, research grants, and public-private partnerships.

Pillar 3: AI-Enhanced Cyber Resilience

This pillar acts as the shield, using AI to strengthen the security of the entire system. It builds on the first two pillars by using real-time threat data and AI tools to proactively detect and prevent cyberattacks. This system requires access to the AI technology and expertise from Pillar 2, as well as data from critical infrastructure. Ethical and legal policies from this pillar are also crucial for ensuring that AI is used responsibly not only in security but across all sectors. This pillar operationalizes the strategies from Pillar 1 by giving them advanced AI tools and, in turn, creates a more resilient environment that makes the broader deployment of AI in Pillar 2 more trustworthy and secure.

The input for the processes in this pillar, include: Real-time Cyber Threat Data, i.e.: constant streams of data on cyberattacks, vulnerabilities, and threat patterns (this data would be shared through the CSIRTs from Pillar 1); AI Technology and Expertise, i.e.: access to the AI tools, algorithms, and expert knowledge developed or acquired through Pillar 2; Ethical and Legal Frameworks, i.e.:

policies and guidelines addressing the use of AI in security, including issues of bias, privacy, and accountability; Incident Response Data, i.e.: Historical data from past cyber incidents to train AI models for better prediction and detection; and Data from Critical Infrastructure, i.e.: data feeds from key economic and government infrastructure (e.g., energy grids, financial systems) for anomaly detection.

The Interconnected Cycle

These three pillars work together in a virtuous cycle. Pillar 1creates the secure foundation, which allows for the safe development of AI in Pillar 2. The AI tools developed in Pillar 2 are then used to enhance the security of the entire system in Pillar 3. This improved security, in turn, makes the environment even more conducive for future technological and economic development. This integrated approach ensures that technology, security, and economic progress are all mutually supportive.

Figure 3 shows the framework diagram for the country.

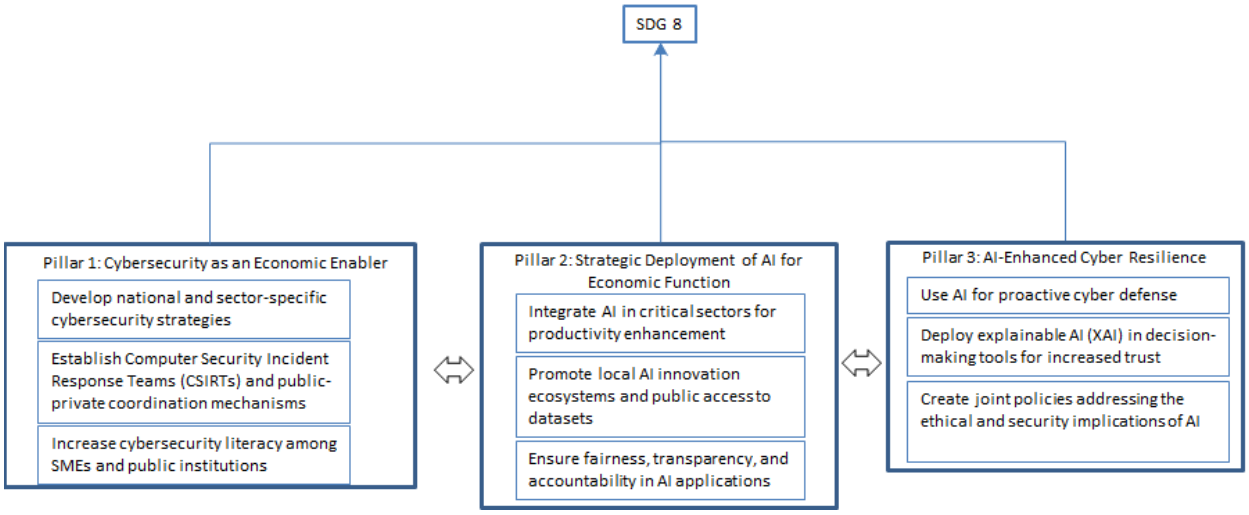

Figure 3. Integrated framework for cybersecurity & AI-Driven economic resilience in developing countries

Case Study Remarks

Sudan's fast-moving digital economy provides fertile ground for a pilot application of the proposed framework. Implementing these strategic cybersecurity and AI interventions can enable Sudan—and similar countries—to not only sustain growth but also shield that growth from digital disruptions, aligning effectively with SDG 8.

Synthesizing Cybersecurity and AI for Resilience

The proposed framework underscores the strategic convergence of cybersecurity infrastructure and AI deployment as essential drivers of economic resilience in developing countries. Traditionally, these domains have been approached separately—cybersecurity as a technical or regulatory concern, and AI as an innovation agenda. However, this siloed approach fails to account for their interdependencies in digital economies, especially those in fragile policy and infrastructure environments.

Cybersecurity provides the trust foundation needed for digital transactions, AI systems, and e-government services to function effectively. Simultaneously, AI offers tools to scale and enhance cyber defense systems, making them more adaptive, predictive, and efficient. When synchronized, the two can significantly reduce digital and economic vulnerabilities.

Addressing Structural Challenges in Developing Countries

Implementing the framework in contexts like Sudan reveals both opportunities and structural constraints:

1. Opportunities include the ability to leapfrog legacy systems, rapidly scale mobile-based AI services, and nurture youth-driven digital entrepreneurship.
2. Constraints involve limited AI research capacity, poor data governance structures, and weak regulatory enforcement for cybersecurity laws.

The solution is not to replicate high-income country models but to adapt policies, technologies, and governance mechanisms to the socio-economic realities of the Global South. This includes fostering multi-stakeholder ecosystems where government, academia, private sector, and civil society co-develop local solutions.

Comparative Analysis of Existing Frameworks

We performed a comparative analysis of selected existing frameworks, i.e.: Digital Transformation for Sustain-able Development (DT4SD), (UNCTAD, 2021); AI for Sustainable Development Framework (AISD), (UNESCO, 2022); National Cyber-security Strategy (NCS), ((ITU, 2020), (World Bank, 2022)); Smart Development Framework (SDF), (Lee & Singh, 2021); and Resilience through Digital Innovation (ReDI), (Gupta, et al., 2023), summarized in Table 3.

Table 3. Comparative Evaluation of Digital Resilience Frameworks

Framework	Primary Objective	AI Integration	Cyber-security Integration	Economic Resilience Focus	Sustainability & Equity Considerations	Applicability to Developing Countries	Key Strengths	Key Limitations
DT4SD (UNCTAD, 2021)	Promote inclusive digital transformation aligned with the SDGs	Moderate: AI is recognized as a tool for innovation and public service delivery, but lacks implementation guidance or technical roadmaps	Low: Cyber risks are acknowledged, but no structured strategy for cyber defense or incident response	Moderate: Links digitalization to economic growth and job creation, especially for SMEs and informal sectors	High: Fully aligned with all 17 SDGs; emphasizes digital inclusion, gender equity, and accessibility	High: Specifically designed for low- and middle-income countries; policy-oriented and scalable	Holistic SDG alignment; strong focus on inclusivity and capacity building	Weak integration of AI and cybersecurity; lacks of technical depth and resilience metrics
AISD (UNESCO, 2022)	Ensure ethical, inclusive, and human-centered deployment of AI in public sectors	High: Comprehensive focus on ethical AI, algorithmic transparency, localization, and public trust; supports AI for education, health, and governance	Low: Cybersecurity mentioned only as a risk (e.g., data breaches), not as a strategic enabler; no technical or institutional	Moderate: Emphasizes innovation and productivity gains, but does not explicitly link AI to economic shock absorption or	High: Strong emphasis on human rights, gender equality, and marginalized communities; promotes participatory AI governance	Medium: Best suited for countries with moderate digital infrastructure and regulatory capacity	Ethical foundation; promotes local ownership and inclusive design	Lacks integration with national security; overlooks cyber resilience as a growth enabler

			integration	crisis response				
NCS Model (ITU, 2020) (World Bank, 2022)	Strengthen national cyber resilience and protect critical infrastructure	Low: AI referenced only in adversarial contexts (e.g., AI-powered cyberattacks), not as a defensive or economic tool	High: Structured framework with five pillars: legal, technical, organizational, capacity building, and cooperation; includes incident response and risk assessment	Moderate: Focuses on continuity of essential services (e.g., finance, energy), contributing indirectly to economic stability	Low: No direct linkage to environmental sustainability or social equity; primarily security-focused	High: Widely adopted across Africa, South Asia, and Latin America; supported by donor funding and technical assistance	Practical, modular, and implementable; strong institutional guidance	Does not leverage AI for proactive defense or economic forecasting; not growth-oriented
SDF (Lee & Singh, 2021)	Leverage AI and IoT to drive economic modernization in emerging markets	High: AI used for smart agriculture, urban planning, healthcare, and market optimization; includes predictive analytics	Medium: Addresses data protection and cyber hygiene, but lacks national-level cyber defense planning or real-time monitoring	High: Explicitly links digital technologies to GDP resilience, SME competitiveness, and productivity growth	Medium: Mentions green technologies and energy efficiency, but lacks SDG-aligned KPIs or equity metrics	Medium: Requires baseline digital infrastructure; more suitable for upper-middle-income nations	Integrates AI with macro-economic modeling; innovation-driven	Assumes high digital maturity; less adaptable to low-resource settings
ReDI (Gupta et al., 2023)	Enhance economic resilience through integrated digital innovation and crisis response	High: AI used for predictive economic modeling, supply chain risk assessment, and post-crisis recovery planning	High: Cyber risk management embedded as a core component of national resilience; includes threat intelligence and adaptive governance	High: Direct focus on economic continuity, adaptive capacity, and recovery from shocks (e.g., pandemics, cyber-attacks)	Medium: Aligned with SDG 9 (industry, innovation) and SDG 17 (partnerships); limited focus on gender or climate equity	High: Designed specifically for emerging economies; modular and scalable	Balanced integration of AI and cybersecurity; policy-action linkage	Limited empirical validation in fragile or conflict-affected states
Proposed Framework	Integrate AI and cybersecurity as co-	High: AI applied to economic forecasting, fraud	High: Cybersecurity treated as foundatio	High: Explicitly links AI-cyber synergy to	High: Embeds SDG-aligned KPIs (SDG	High: Modular, context-sensitive, and	Holistic, integrates technology, policy, sustainabilit	Requires stakeholder coordination and

	enablers of sustain-able and resilient economi c growth	detection, automation, and market intelligence ; supports local AI model developme nt	nal to digital trust, infra-structure integrity, and financial system stability	long-term economic stability, SME resilience, and shock absorption	8, 9, 10, 13); prioritize s gender inclusion, green AI, and environ-mental impact	scalable across income levels; supports mobile-first and low-bandwidth solutions	y, and equity; designed for real-world implementa tion in resource-constrained settings	pilot testing for validatio n

Alignment with the SDG Agenda

The framework aligns closely with SDG 8 (Decent Work and Economic Growth) by enabling:

1. Job creation in cybersecurity and AI-related industries.
2. Resilience of SMEs and digital services to cyber threats.
3. Inclusiveness through AI-driven tools for agriculture, health, and finance, particularly for rural populations and marginalized communities.

Moreover, its design supports SDG 9 (Industry, Innovation, and Infrastructure) and SDG 16 (Peace, Justice, and Strong Institutions) by building digital trust and enhancing governance capacity.

Risks and Ethical Considerations

The integration of AI and cybersecurity is not without risk. AI systems can be biased, non-transparent, and used for surveillance. Cybersecurity regimes can become overly centralized or authoritarian. To mitigate these concerns:

1. Governments should adopt AI ethics principles, including fairness, accountability, and transparency (FAT).
2. Civil society should be engaged in technology governance, ensuring that digital tools serve democratic and inclusive goals.

Ethical and contextual adaptation must remain central to implementation.

Features as novelty of the proposed framework

Table 4 shows the features of the proposed framework along with their rationale of the framework's novelty.

Table 4. features of the proposed framework

Feature	Rational
1. AI & Cybersecurity as Co-Enablers	First framework to treat AI and cybersecurity as interdependent pillars of economic resilience—not isolated domains.
2. Built for Economic Resilience	Focuses on absorbing shocks (e.g., cyberattacks, pandemic, market crash.)
3. Embedded Sustainability & Equity	Integrates SDG-aligned KPIs (e.g., green AI, gender inclusion.)
4. Modular & Context-Sensitive	Adaptable to low-resource settings (e.g., SMS-based AI, lightweight encryption); scalable as capacity grows.
5. Anticipatory Governance	Uses AI for predictive analytics (e.g., forecasting financial instability or cyber threats—before they escalate.)
6. Digital Trust as a Public Good	Positions cybersecurity as foundational to financial inclusion on e-government and SME participation.

CONCLUSION

This paper presented a conceptual framework positioning cybersecurity and artificial intelligence (AI) as pivotal enablers of economic resilience and sustainable growth in developing countries. Grounded in the principles of the Sustainable Development Goals—especially SDG 8—the framework integrates cybersecurity infrastructure, AI-driven economic transformation, and AI-enhanced cyber defense to address systemic vulnerabilities in digital economies. The case study of Sudan illustrated how context-specific adaptations of this framework can support the rapid digitalization of economies while safeguarding critical infrastructure and fostering inclusive growth. However, the framework's success hinges on multi-stakeholder collaboration, capacity building,

ethical governance, and continuous policy innovation. The convergence of cybersecurity and AI presents a strategic opportunity for developing countries to enhance their economic resilience. By adopting a comprehensive framework that integrates these elements with SDG 8, nations can navigate the complexities of digital transformation while fostering inclusive and sustainable economic growth.

Future research must empirically validate this framework across diverse developing country settings and explore the nuanced socio-technical dynamics of AI and cybersecurity adoption. Ultimately, this integrative approach holds promise for leveraging digital transformation as a resilient foundation for economic prosperity in the Global South. In addition, this study lays the groundwork for several future research and policy agendas:

1. Empirical validation of the framework in multiple countries (e.g., through case studies or longitudinal assessments).
2. Quantitative modeling to link investments in cybersecurity/AI to GDP growth or digital trust indices.
3. Policy experimentation involving regulatory sandboxes for AI in sectors like health, finance, or e-commerce.

Such research will help to move from theoretical frameworks to evidence-based policy interventions.

AUTHOR CONTRIBUTIONS

A.S.M.: method conceptualization, simulation, and initial article writing. R.B.: method conceptualization and finalizing article.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

Brundage, M., Avin, S., Clark, J., et al. (2018). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. *arXiv preprint,* 2004.07213. https://doi.org/10.48550/arXiv.2004.07213

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

Carlson, J., & Chaturvedi, A. (2019). Cybersecurity and sustainable development: Challenges and opportunities. *Journal of Cyber Policy*, 4(2), 173–189. https://doi.org/10.1080/23738871.2019.1636602

Chu, A. B. (2018). Mobile Technology and Financial Inclusion. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1, Cryptocurrency, FinTech, InsurTech, and Regulation* (pp. 131–144). Academic Press. https://doi.org/10.1016/B978-0-12-810441-5.00006-3

Cummings, M. (2020). AI ethics and policy in developing countries: Challenges and opportunities. *AI & Society*, 35(3), 589–601. https://doi.org/10.1007/s00146-020-00962-3

DATAREPORTAL, (2025). *Digital Sudan-2025*, Retrieved from https://datareportal.com/reports/digital-2025-sudan

Gupta, S., Arora, P., & Nkosi, M. (2023). Resilience through digital innovation: A framework for integrating AI and cybersecurity in emerging economies. *Sustainable Development*, 31(4), 2105–2120. https://doi.org/10.1002/sd.2456

ITU, (2020). *Marrying artificial intelligence and the sustainable development goals: the global economic impact of AI*. Retrieved from https://www.itu.int/hub/2020/04/marrying-artificial-intelligence-and-the-sustainable-development-goals-the-global-economic-impact-of-ai/

ITU. (2020). *Guide to developing a national cybersecurity strategy (2nd ed.)*. International Telecommunication Union. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Guide-to-National-Cybersecurity-Strategy.aspx

ITU, (2023). *Cybersecurity readiness index: measuring capacity in the global south*. Retrieved from https://www.itu.int

ISPAR, (2024). *Global Cybersecurity Index*, Retrieved from https://sudan.unescwa.org/ISPAR/

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.08.002

Kshetri, N. (2021). AI and cybersecurity in developing countries: Challenges and prospects. *Information & Management*, 58(4), 103464. https://doi.org/10.1016/j.im.2021.103464

Kumar, S., Sinha, A., & Singh, A. (2021). Cybersecurity challenges in developing countries: A review. *International Journal of Information Management*, 57, 102319. https://doi.org/10.1016/j.ijinfomgt.2020.102319

Lee, J., & Singh, R. (2021). Smart development: Integrating AI and IoT for economic transformation in emerging markets. *Technological Forecasting and Social Change*, 168, 120789. https://doi.org/10.1016/j.techfore.2021.120789

Mendes, C., & Rios, T. N. (2023). Explainable artificial intelligence and cybersecurity: a systematic literature review. arXiv. Retrieved from https://arxiv.org/abs/2303.01259

Modern Diplomacy. (2024). *Strengthening cyber defences in developing countries: offensive and adversarial ai threats*. Retrieved from https://moderndiplomacy.eu/2024/07/15/strengthening-cyber-defences-in-developing-countries-offensive-and-adversarial-ai-threats/

Nakamura, T., & Harada, T. (2020). Cyber resilience in the digital age: Strategies for developing countries. *Information Security Journal: A Global Perspective*, 29(4), 153–165. https://doi.org/10.1080/19393555.2020.1747370

NCSI, (2023), *National Cyber Security Index*, Retrieved from https://ncsi.ega.ee/ncsi-index/

Nguyen, T., & Nguyen, T. (2022). AI-based cybersecurity solutions for emerging economies. *Cybersecurity*, 5(1), 12. https://doi.org/10.1186/s42400-022-00099-4

OECD. (2021). Enhancing cybersecurity for digital transformation in developing countries. *OECD Digital Economy Outlook*. Retrieved from https://doi.org/10.1787/ed3e4b1e-en

Oxford Insights, (2024). *AI Readiness Rank*. Retrieved from https://oxfordinsights.com/ai-readiness/ai-readiness-index/

PwC (2020). *AI predictions: The global economic impact of AI by 2030*. Retrieved from https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Raghavan, S., & Mulder, K. (2021). Building global cyber resilience: Policy frameworks and stakeholder engagement. *Journal of Cybersecurity Policy & Practice*, 3(2), 233–249. https://doi.org/10.1177/25166026211008474

Szegedy, C., Ioffe, S., & Vanhoucke, V. (2019). Analyzing adversarial examples in cybersecurity. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* pp. 4472–4481. Long Beach, LA, USA.

UNCTAD. (2019). *Digital economy report 2019: Value creation and capture—Implications for developing countries*. United Nations. Retrieved from https://unctad.org/webflyer/digital-economy-report-2019

UNCTAD. (2021). *Digital transformation for sustainable development: A guide for policymakers in developing countries*. United Nations Conference on Trade and Development. Retrieved from https://unctad.org/publication/digital-transformation-sustainable-development

UNESCO. (2022). *AI and the futures of education: Ethical and inclusive pathways for sustainable development*. United Nations Educational, Scientific and Cultural Organization. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000382395

UNDP. (2022). *Digital transformation for sustainable development: A framework for action*. United Nations Development Programme.

United Nation, (2020). *Sustainable Development Goals*, Retrieved from https://www.un.org/sustainabledevelopment/economic-growth/

World Bank. (2020). *World development report 2020: Trading for development in the age of global value chains*. World Bank Publications.

World Bank. (2023). *Cybersecurity economics for emerging markets*. Retrieved from https://www.worldbank.org

World Bank. (2025). *Cybersecurity economics*. Retrieved from https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets

World Economic Forum. (2020). *The global risks report 2020*. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020

Zhou, Y., Li, X., & Wang, L. (2022). AI-driven policy frameworks for cybersecurity resilience. *AI & Society*, 37(1), 123–137. Retrieved from https://doi.org/10.1007/s00146-022-01455-8