African Journal of Economics and Sustainable Development

ISSN: 2689-5080

Volume 8, Issue 1, 2025 (pp. 95-104)

www.abjournals.org

SECURING CROSS-BORDER DIGITAL TRADE: AI STRATEGIES FOR EU-AFRICA ECONOMIC GROWTH

Anya Adebayo Anya[1], Kelechi Adura Anya[2], Eke Kehinde Anya[3],

and Akinwale Victor Ishola[4]

[1]Department of Political Science, Obafemi Awolowo University, Ile-Ife.
Email: adeanya@summalogix.com

[2]Computer Science, Landmark University, Omu-Aran, Nigeria.
Email: anyakelechiadura@gmail.com

[3]Scottish Power Headquarters, Glasgow.
Email: eanya@spenergynetworks.co.uk

[4]Department of Peace, Security and Humanitarian Studies, University of Ibadan.
Email: victorakinwale2@gmail.com

Cite this article:

Anya, A. A., Anya, K. A., Anya, E. K., Ishola, A. V. (2025), Securing Cross-Border Digital Trade: AI Strategies for Eu-Africa Economic Growth. African Journal of Economics and Sustainable Development 8(1), 95-104. DOI: 10.52589/AJESD-VKCUF5DN

Manuscript History

Received: 19 Nov 2024

Accepted: 30 Jan 2025

Published: 18 Feb 2025

ABSTRACT: *The rapid growth of cross-border digital trade has transformed economic interactions between regions, with the European Union (EU) and African economies playing critical roles in this evolving landscape. As a driver of innovation, economic growth, and regional integration, digital trade presents significant developmental opportunities. However, the proliferation of cybersecurity threats undermines trust in digital transactions and poses challenges to the sustainability of cross-border digital trade. These risks are exacerbated by regional disparities in cybersecurity readiness, infrastructure, and regulatory frameworks, highlighting the need for robust, innovative approaches to ensure secure and resilient digital trade ecosystems. This paper explores the potential of Artificial Intelligence (AI) as a strategic tool to mitigate cybersecurity risks and foster secure trade between the EU and Africa. The study examines the defining characteristics and economic significance of cross-border digital trade, emphasizing its role in fostering economic partnerships between the EU and Africa. It highlights existing trade agreements, collaborative efforts, and the projected growth of digital economies in both regions. Despite these opportunities, cybersecurity threats, such as data breaches, ransomware attacks, and phishing scams, present significant economic and operational challenges. The study underscores the disparities in cybersecurity preparedness, particularly in the African context, and their implications for sustainable digital trade growth. The role of Artificial Intelligence in enhancing cybersecurity is critically analyzed, focusing on its applications in threat detection, predictive analytics, anomaly identification, and automated incident response. Drawing on successful case studies, the paper demonstrates the transformative potential of AI in addressing complex cybersecurity challenges and strengthening the resilience of digital trade infrastructures. By leveraging AI-driven solutions, the EU and African economies can establish secure digital ecosystems, fostering trust and enhancing economic collaboration. The paper concludes with targeted recommendations to enhance cybersecurity in cross-border digital trade. Policy measures, such as harmonizing cybersecurity regulations and promoting AI-driven research and innovation, are essential for building a cohesive security framework. Technological investments in AI infrastructure and the development of shared cybersecurity platforms are equally vital. Furthermore, capacity-building initiatives, including specialized training programs for businesses and governments, are necessary to ensure effective implementation. These recommendations aim to address the cybersecurity challenges of cross-border digital trade and advance a secure, inclusive, and sustainable digital economy between the EU and Africa.*

KEYWORDS: Cross-border, Digital trade and AI.

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

INTRODUCTION

Over the past few decades, the digital revolution has significantly reshaped global commerce, unlocking new possibilities for international transactions. Digital trade, defined by the cross-border exchange of goods, services, and data through digital platforms, has become a key catalyst for economic growth and innovation. The internet has revolutionized the production, delivery, and consumption of goods and services worldwide, paving the way for innovative business models and international transactions (Meltzer, 2016; Vitaash & Shah, 2018). Within the European Union (EU) and African economies, digital trade offers distinctive prospects for enhancing cooperation, broadening market access, and tackling developmental issues. Nonetheless, as digital ecosystems grow more interconnected, they face escalating cybersecurity risks that can erode trust, disrupt trade operations, and hinder economic advancement.

Cybersecurity threats, including data breaches, ransomware attacks, and phishing scams, have emerged as widespread challenges in the digital economy. These issues are especially significant in cross-border digital trade, where differences in regulatory systems, unequal technological infrastructure, and the extensive volume of data exchanges exacerbate vulnerabilities. For both the EU and African economies, securing digital trade is not just a technical requirement but a strategic priority to protect economic benefits and sustain trust among trading partners.

Artificial Intelligence (AI) provides innovative solutions to address the escalating cybersecurity challenges in cross-border digital trade. By analyzing large datasets, identifying anomalies, and responding to threats in real time, AI can significantly enhance cybersecurity measures. Utilizing AI-powered strategies can bolster the resilience of digital trade systems, reduce risks, and promote a secure and prosperous digital economy between the EU and Africa.

While cross-border digital trade holds immense potential to spur economic development and foster partnerships, it remains highly susceptible to cybersecurity threats. Issues such as data breaches, ransomware attacks, and phishing scams threaten the integrity, confidentiality, and reliability of digital trade systems. These risks are intensified by disparities in cybersecurity preparedness across regions, fragmented regulatory frameworks, and limited capacity to counter advanced cyber threats. For the EU and African economies, such vulnerabilities endanger not only specific transactions but also the broader economic stability and trust essential for the long-term growth of digital trade.

Moreover, the increasing complexity and magnitude of cyber threats require innovative approaches beyond the scope of traditional cybersecurity measures. The absence of harmonized policies and collaborative frameworks between the EU and African economies further impedes efforts to safeguard digital trade pathways. Without effective mechanisms to manage these risks, the economic and developmental advantages of digital trade could be compromised, jeopardizing the vision of a secure and inclusive digital economy.

Artificial Intelligence (AI) offers innovative solutions to address the escalating cybersecurity challenges in cross-border digital trade. Its capacity to process large volumes of data, identify anomalies, and respond to threats in real time positions AI as a crucial tool for reinforcing cybersecurity frameworks. Implementing AI-driven strategies can fortify digital trade infrastructures, reduce vulnerabilities, and support the development of a secure and flourishing digital economy between the EU and Africa. This paper explores the significance of securing

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

cross-border digital trade and highlights AI strategies as a cornerstone for mitigating cybersecurity threats. By examining existing challenges, showcasing the potential of AI solutions, and providing actionable recommendations, this paper aims to contribute to a robust and secure digital trade ecosystem that supports economic growth and strengthens the partnership between the EU and African economies.

OVERVIEW OF CROSS-BORDER DIGITAL TRADE

Cross-Border Digital Trade

The rise of cross-border digital trade, encompassing e-commerce and the delivery of digital products, has emerged as a dominant force in global commerce, driven by advancements in digital technologies (Qu, 2020). This transformation is not just reshaping how businesses engage in trade, but also how economies globally operate. Digital trade enables companies to transcend geographical borders, facilitating transactions in real-time and lowering the barriers to market entry for businesses of all sizes. In this digital era, e-commerce platforms and the delivery of digital services are becoming central pillars of international trade, with increasing participation by businesses worldwide (Smirnov, 2019). The speed at which digital trade has expanded presents both opportunities and challenges, as countries, particularly emerging economies such as China, work to adapt to this fast-evolving landscape (Gao, 2024).

At the heart of this evolution are innovations such as smart contracts, which have revolutionized cross-border transactions. Smart contracts, powered by blockchain technology, automate and enforce the terms of an agreement between parties, thereby reducing the need for intermediaries (Hourani, 2017). This automation not only streamlines transactions but also enhances their security, making cross-border digital trade more efficient and trustworthy. However, while smart contracts and other technological advancements offer tremendous potential for enhancing trade efficiency, they also raise concerns around cybersecurity, regulatory standards, and the legal enforceability of digital agreements across jurisdictions. The complexity of these issues calls for sophisticated and coordinated global responses to ensure the long-term success of cross-border digital trade.

As digital trade continues to reshape traditional exchange patterns, it offers numerous opportunities, particularly for small- and medium-sized enterprises (SMEs) that may have been previously excluded from global trade (Smirnov, 2019; Qu, 2020). The digitalization of trade lowers transaction costs and enables SMEs to access vast global markets via digital platforms. This democratization of commerce has the potential to create a more inclusive global economy, where businesses, regardless of their size or location, can compete on a more level playing field. However, this shift also presents significant challenges. The increased volume of cross-border transactions, coupled with the rapid pace of technological innovation, means that regulatory frameworks and cybersecurity measures must evolve to keep pace with new risks and complexities.

For countries like China, the rise of cross-border digital trade has prompted the need for strategic adaptations in policies and infrastructure to manage both the opportunities and challenges this shift presents (Gao, 2024). China’s strategic focus on expanding its e-commerce ecosystem, particularly through initiatives like the Belt and Road Initiative, underscores the nation's commitment to integrating digital trade into its broader economic strategy. Yet, the

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

country's efforts also highlight the challenges of harmonizing regulations, addressing cybersecurity concerns, and creating a competitive edge in an increasingly interconnected global digital economy.

The continued expansion of cross-border digital trade is poised to fundamentally transform international economic relations, fostering greater interdependence among nations and establishing a new paradigm for global commerce. As this evolution unfolds, it presents substantial opportunities for economic growth, innovation, and increased inclusivity. However, it also necessitates addressing a range of critical challenges, including the harmonization of regulatory frameworks, enhancing cybersecurity measures, and effectively managing technological advancements such as blockchain and artificial intelligence. In navigating this rapidly evolving landscape, countries must implement forward-looking policies that carefully balance the potential advantages of digital trade with the associated risks, ensuring the development of a secure, inclusive, and sustainable global digital economy.

EU-Africa Digital Trade Relations

The EU-Africa trade relationship has undergone a significant transformation, evolving from a legacy of colonialism to contemporary, formalized agreements that focus on enhancing economic partnerships, particularly in the area of digital trade. Historically, the relationship between the European Union (EU) and Africa was shaped by colonial ties and the subsequent establishment of trade agreements aimed at facilitating economic cooperation. In recent years, however, there has been a shift towards focusing on digital trade as a means to enhance bilateral economic relations, with both regions exploring new avenues for collaboration in this rapidly evolving sector (Adetula & Osegbue, 2020).

The EU has made notable strides in addressing digital trade through its Free Trade Agreements (FTAs), which include provisions for e-commerce and digital services. However, significant challenges remain in ensuring the efficient and seamless flow of data across borders. Micallef (2019) highlighted the regulatory barriers that persist, especially in relation to data protection laws, differing privacy standards, and the logistical challenges of cross-border data flows. These barriers impede the potential for a fully integrated digital trade ecosystem between the EU and African nations, limiting the realization of digital trade’s full economic potential.

Economic Partnership Agreements (EPAs) between the EU and African countries have also played a pivotal role in shaping trade relations, particularly by addressing key development issues such as poverty alleviation, sustainable growth, and rules of origin for products traded between the two regions (Ngangjoh-Hodu & Matambalya, 2009). These agreements are instrumental in fostering deeper economic ties, but there is an increasing need to adapt them to the demands of the digital economy. As digital trade becomes a more central component of the global economy, the need for EPAs to address digital infrastructure, digital literacy, and policy alignment has become more pressing.

The importance of digital trade between the EU and Africa is underscored by recent research that suggests substantial economic growth potential in the sector. According to Teevan and Shiferaw (2023), the digital economy in Africa is expected to reach $180 billion by 2030, making a significant contribution to the realization of the African Continental Free Trade Area (AfCFTA). This growth is seen as a critical element in enhancing intra-African trade and facilitating Africa's integration into the global digital economy. As such, the EU and African countries stand to benefit significantly from a more robust digital trade partnership that capitalizes on these projected advancements.

Moreover, the digital economy is increasingly recognized as a key driver of economic growth in Africa, with the potential to boost productivity, innovation, and job creation. Abendin and Duan (2021) argued that the digital economy plays a vital role in amplifying the positive impacts of international trade on Africa's economic development. By facilitating easier access to markets, fostering innovation, and supporting the growth of digital platforms, the digital economy can help African countries overcome traditional trade barriers and improve their competitive position in global markets.

While significant progress has been made in formalizing EU-Africa trade relations, the full potential of digital trade remains untapped due to a range of challenges. To foster a more integrated and mutually beneficial relationship, both the EU and African nations must prioritize overcoming regulatory hurdles, harmonizing digital policies, and investing in the necessary infrastructure and skills development to support the growth of digital trade. This will not only benefit the economies of both regions but also contribute to broader goals of development, poverty reduction, and economic integration in Africa.

Cybersecurity Threats in Cross-Border Digital Trade

Cybersecurity threats in cross-border digital trade are becoming an increasingly critical concern as the rapid expansion of global data flows and digital technologies enhances connectivity while simultaneously heightening the vulnerability of digital ecosystems to cyberattacks. As highlighted by Meltzer (2020), the growth of the digital economy and the increasing reliance on digital trade have made countries and businesses more susceptible to a range of cybersecurity challenges. Among the most common threats are data breaches, ransomware attacks, and phishing scams, all of which pose substantial risks to both private enterprises and governments in managing the risks associated with transnational digital trade. These threats undermine the confidentiality, integrity, and availability of critical data, making it essential for stakeholders to adopt robust cybersecurity frameworks to safeguard their digital trade activities (Huang et al., 2021).

The cross-border nature of digital trade introduces another layer of complexity, as governments and corporations must navigate a variety of domestic privacy and cybersecurity laws that differ significantly across jurisdictions. Laidlaw (2021) noted that these variations can create significant barriers to the free flow of data, hindering the growth of international digital trade. For instance, stringent data protection regulations in the EU, such as the General Data Protection Regulation (GDPR), impose strict guidelines on how personal data should be handled, creating friction in cross-border data exchanges. Conversely, some African countries, still developing their digital infrastructure, may lack sufficient regulatory frameworks to protect against data breaches and cybercrimes, compounding the risks in digital transactions.

The risks posed by cybersecurity threats in cross-border digital trade are particularly significant for both EU and African economies, given the critical role of digital technologies in driving economic growth, innovation, and competitiveness. Vasiu and Vasiu (2018) emphasized that cybersecurity threats can lead to a wide range of detrimental outcomes, including the theft of trade secrets, financial losses from payment fraud, and damage to the reputation of businesses and governments involved in digital trade. The potential for significant economic damage necessitates the development of comprehensive cybersecurity strategies to ensure the resilience and sustainability of digital trade ecosystems. Both regions must invest in strengthening their cybersecurity infrastructures, enhance collaborative efforts to mitigate cross-border threats, and ensure that their legal frameworks are aligned to enable secure digital transactions.

In Africa, the challenges to e-commerce adoption are compounded by limited ICT infrastructure, low digital literacy rates, and the increasing prevalence of cybercrime. Ndonga (2012) highlighted that these barriers hinder the ability of African countries to fully participate in and benefit from the opportunities provided by digital trade. Moreover, as African countries are increasingly targeted by cybercriminals, there is a pressing need for a more robust regional cybersecurity framework. The African Union (AU) has taken a step in this direction by establishing a regional cybersecurity treaty aimed at addressing these challenges. However, as Orji (2018) pointed out, the slow pace of treaty ratification and the lack of effective coordination between African nations have hindered its implementation, limiting its ability to provide a comprehensive solution to the region's cybersecurity challenges.

The gap in cybersecurity awareness and training programs between Africa and other regions such as the U.S. further exacerbates the challenges faced by African economies in securing their digital trade activities. Popoola et al. (2024) noted that differences in cultural contexts, levels of digital literacy, and the state of technological infrastructure contribute to these disparities. While the U.S. has advanced cybersecurity education and widespread awareness programs, many African countries still struggle with limited access to such resources, exacerbating the vulnerability of their digital systems to cyber threats. To bridge this gap, it is essential that African nations prioritize investment in cybersecurity education, awareness campaigns, and training programs to build capacity at both the governmental and private sector levels.

Cybersecurity remains a significant threat to the continued growth and development of cross-border digital trade, particularly for EU and African economies. Addressing these challenges requires a multifaceted approach, including strengthening legal frameworks, enhancing digital infrastructure, increasing cybersecurity awareness and training, and fostering greater international cooperation to combat transnational cybercrime. Only through such efforts can the EU and Africa secure their digital trade systems and unlock the full potential of the digital economy.

Role of Artificial Intelligence in Mitigating Cybersecurity Risks

Artificial Intelligence (AI) has emerged as a transformative tool in the fight against cybersecurity threats, providing advanced solutions for threat detection, vulnerability assessment, incident response, and predictive analysis. As highlighted by Camacho (2024) and Thapaliya and Bokani (2024), AI technologies, particularly machine learning algorithms, are revolutionizing the cybersecurity landscape by enabling the swift analysis of vast amounts of data to detect anomalous patterns that could signify potential security breaches. These capabilities allow for a more proactive and efficient defense against the increasingly sophisticated cyber threats facing organizations globally.

The application of AI in cybersecurity includes real-time threat detection, where machine learning models are trained to identify patterns in network traffic, user behavior, and system activity that may indicate an ongoing attack (Camacho, 2024). By continuously analyzing this data, AI systems can quickly detect vulnerabilities before they are exploited, offering a significant advantage over traditional, manual methods of threat identification. Furthermore,

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

AI's ability to predict potential future attacks through predictive analytics allows organizations to take preventative measures, thus enhancing overall security posture (Camacho, 2024; Jimmy, 2021).

AI-driven technologies also play a crucial role in automating incident response, significantly reducing response times and minimizing the impact of security breaches. With automated processes, AI systems can quickly contain threats, initiate remediation actions, and mitigate damage without the need for human intervention, ensuring that security incidents are addressed in real-time (Thapaliya & Bokani, 2024). This capacity to automate incident response also alleviates the burden on security teams, allowing them to focus on more complex tasks while AI handles routine security processes.

In both the EU and Africa, AI is being increasingly adopted as part of cybersecurity strategies. In Africa, for instance, approximately 69.16% of companies have implemented information security strategies, with 45% of them integrating AI-based technologies into their security frameworks (Nibigira et al., 2024). This adoption highlights the growing recognition of AI's role in enhancing cybersecurity defenses and responding to the unique challenges faced by African businesses in an increasingly digital and interconnected environment. The use of AI for cybersecurity in Africa aligns with the global trend of leveraging advanced technologies to protect against cyber threats, ensuring that organizations can maintain the confidentiality, integrity, and availability of their systems and data.

The role of AI in mitigating cybersecurity risks cannot be overstated. As cyber threats continue to evolve in complexity, AI offers a powerful means of addressing these challenges by enhancing threat detection, automating incident response, and providing predictive capabilities that empower organizations to take a proactive approach to cybersecurity. Its integration into cybersecurity strategies in both the EU and Africa underscores its importance as a tool for safeguarding digital assets and ensuring the stability and resilience of digital economies.

Recommendations for Enhancing Cybersecurity in Cross-Border Digital Trade

The increasing complexity of cross-border digital trade, alongside the escalating cybersecurity risks it entails, necessitates robust strategies to protect the integrity and security of digital infrastructures. As digital trade continues to expand, particularly between the EU and African nations, cybersecurity becomes a critical concern that requires coordinated efforts at the policy, technological, and capacity-building levels. This section presents a set of recommendations to strengthen cybersecurity in cross-border digital trade, addressing policy frameworks, technological advancements, and capacity-building initiatives.

POLICY RECOMMENDATIONS

1. Harmonizing Cybersecurity Policies and Regulations Between the EU and African Nations

One of the most pressing challenges in enhancing cybersecurity within cross-border digital trade is the lack of regulatory harmonization between different regions. Inconsistent cybersecurity standards and regulatory frameworks between the EU and African nations create barriers to secure data flows, complicating the management of transnational cyber risks

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

(Laidlaw, 2021). To mitigate these challenges, it is essential for both regions to align their cybersecurity policies and regulations.

A unified regulatory approach would streamline processes for cross-border data transfers, facilitate collaboration on cybersecurity initiatives, and improve the overall security of digital trade transactions. Efforts should focus on creating bilateral or multilateral agreements that establish common cybersecurity standards, rules of origin for digital products, and data privacy protections that are adaptable to the diverse legal environments in both regions (Micallef, 2019). Additionally, the establishment of a joint EU-Africa cybersecurity task force could enhance information sharing and best practices between the two regions, fostering greater collaboration in addressing emerging threats.

2. Incentivizing AI-Driven Cybersecurity Research and Innovation

The integration of Artificial Intelligence (AI) in cybersecurity offers immense potential for addressing the sophisticated nature of modern cyber threats (Camacho, 2024). Both the EU and African countries should prioritize incentivizing AI-driven research and innovation in the cybersecurity field. Governments and private sector entities should collaborate to fund AI-focused cybersecurity research, particularly projects that explore the application of machine learning algorithms, predictive analytics, and automation in threat detection and incident response.

Establishing innovation hubs and funding programs for AI-driven cybersecurity startups could spur the development of new technologies and solutions tailored to the specific cybersecurity needs of cross-border digital trade. Furthermore, encouraging collaboration between academia, industry, and government agencies in both the EU and Africa can accelerate the deployment of AI-driven solutions across digital platforms, ensuring that businesses are equipped with the necessary tools to protect themselves against evolving threats.

Technological Recommendations

1. Investment in AI Infrastructure and Capacity Building

To effectively implement AI-driven cybersecurity solutions, substantial investment in AI infrastructure is required. Both the EU and African countries should focus on building robust AI ecosystems that can support the development and deployment of advanced cybersecurity technologies. This includes investing in the necessary hardware, such as high-performance computing systems, and software platforms that enable the processing and analysis of large datasets in real time.

Moreover, it is essential to foster capacity-building initiatives that equip both public and private sector organizations with the skills and knowledge necessary to implement AI-based cybersecurity solutions effectively. In Africa, where technological infrastructure and digital literacy levels are varied, targeted investments in AI infrastructure could help bridge the digital divide and ensure that AI-driven cybersecurity solutions are accessible across the continent (Nibigira et al., 2024). The EU should also leverage its existing technological capabilities to support Africa in building a strong AI infrastructure, promoting knowledge transfer and capacity development in the process.

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN

2. Development of Shared Cybersecurity Platforms Powered by AI

A critical technological recommendation for enhancing cybersecurity in cross-border digital trade is the development of shared cybersecurity platforms powered by AI. These platforms could provide a unified approach to threat detection, incident response, and information sharing between EU and African nations. Such platforms would leverage AI technologies to analyze cross-border data flows and detect cybersecurity threats in real time, enhancing the ability of both regions to respond quickly to emerging risks.

These shared platforms could also serve as collaborative spaces where businesses, governments, and cybersecurity experts from both regions can share threat intelligence and cybersecurity best practices. In addition to strengthening regional security, this approach would also help to foster greater cooperation between the EU and African nations, promoting trust and resilience in digital trade ecosystems. Developing shared platforms would not only increase the efficiency of cybersecurity measures but also create an environment conducive to the seamless exchange of goods, services, and data across borders.

Capacity-Building Initiatives

1. Training Programs for Businesses and Governments on AI Cybersecurity Solutions

To fully capitalize on the potential of AI in enhancing cybersecurity, targeted training programs are essential for both businesses and governments. These programs should focus on equipping stakeholders with the skills necessary to implement and manage AI-driven cybersecurity solutions effectively. For businesses, particularly small and medium-sized enterprises (SMEs) in Africa, which often lack the resources to invest in robust cybersecurity measures, affordable training and support programs, are critical. These initiatives should emphasize practical applications of AI technologies in securing digital trade transactions and protecting sensitive data.

Governments in both the EU and Africa should also invest in cybersecurity training for public sector employees, particularly those involved in regulatory enforcement and policymaking. Governments play a central role in the development and implementation of cybersecurity regulations, and ensuring that officials are well-versed in AI-driven cybersecurity technologies will allow them to create informed policies and provide appropriate guidance to businesses.

In Africa, where digital literacy remains a challenge in certain regions, governments should prioritize the development of digital literacy programs as part of broader educational reforms. Training programs should be designed to be inclusive and accessible, targeting various levels of expertise to ensure that all stakeholders are prepared to engage with advanced cybersecurity technologies.

REFERENCES

Abendin, S., & Duan, P. (2021). International trade and economic growth in Africa: The role of the digital economy. *Cogent Economics & Finance, 9*.

Adetula, V.A., & Osegbue, C. (2020). Trade and the Economic Partnership Agreements in EU-Africa relations.

Camacho, N.G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General science (JAIGS) ISSN:3006-4023*.

Gao, X. (2024). Research on the Development Strategy of Cross-border E-commerce in China Under the Background of Digital Trade. *International Journal of Education and Humanities*.

Hourani, S. (2017). Cross-border smart contracts: boosting international digital trade through trust and adequate remedies.

Huang, K., Madnick, S.E., Choucri, N., & Zhang, F. (2021). A Systematic Framework to Understand Transnational Governance for Cybersecurity Risks from Digital Trade. *Global Policy*.

Jimmy, F. (2021). Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses. *International Journal of Scientific Research and Management (IJSRM)*.

Laidlaw, E.B. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. *Social Science Research Network*.

Meltzer, J.P. (2016). Maximizing the Opportunities of the Internet for International Trade. *Economics of Networks eJournal*.

Meltzer, J.P. (2020). Cybersecurity, Digital Trade, and Data Flows: Re-thinking a Role for International Trade Rules. *SSRN Electronic Journal*.

Micallef, J.A. (2019). Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential? *Journal of World Trade*.

Ndonga, D. (2012). E-Commerce in Africa: Challenges and Solutions. *African Journal of Legal Studies, 5*, 243-268.

Ngangjoh-Hodu, Y., & Matambalya, F.A. (2009). Trade relations between the EU and Africa : development, challenges and options beyond the Cotonou Agreement.

Nibigira, N., Havyarimana, V., & Xiao, Z. (2024). Artificial Intelligence Adoption for Cybersecurity in Africa. *Journal of Information Security*.

Orji, U.J. (2018). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology*.

Popoola, O.A., Akinsanya, M.O., Nzeako, G., Chukwurah, E.G., & Okeke, C.D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives. *International Journal of Applied Research in Social Sciences*.

Qu, X. (2020). Research on the Development of Cross-Border E-commerce in the Context of Digital Trade. *Proceedings of the 2020 2nd International Conference on Economic Management and Cultural Industry (ICEMCl 2020)*.

Smirnov, E.N. (2019). Parameters of development and regulation of the international digital trade at the present stage. *E-Management*.

Teevan, C., & Shiferaw, L.T. (2023). Digital geopolitics in Africa: Moving from strategy to action.

Thapaliya, S., & Bokani, A. (2024). Leveraging artificial intelligence for enhanced cybersecurity: insights and innovations. *SADGAMAYA*.

Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. *SRPN: Globalization (Sustainability) (Topic)*.

vitaash, K., & Shah, A. (2018). Maximizing the Opportunities of the Internet for International Trade. *TIJ's Research Journal of Economics & Business Studies - RJEBS, 8*.

Article DOI: 10.52589/AJESD-VKCUF5DN
DOI URL: https://doi.org/10.52589/AJESD-VKCUF5DN