MSI Journal of
AI and Technology

The Effect of Cybercrime on Digital Economy Growth: A Global Analysis

Arif Mainuddin[1*], Md. Nazmul Huda Masud[2], Tamjid Mohd Imrul Ibrahim[3], Rafsan Anwar[4], Md. Mehedi Hasan Babu[5]

[1*] Police Staff College Bangladesh, Bangladesh.

[2] University of Dhaka, Bangladesh.

[3] International Islamic University Chittagong, Bangladesh.

[4] United International University, Bangladesh.

[5] United International University, Bangladesh.

*** Correspondence:** Arif Mainuddin

The authors declare that no funding was received for this work.

OPEN ACCESS

Received: 10-December-2025

Accepted: 19-January-2026

Published: 25-January-2026

This article is published in the **MSI Journal of AI and Technology**,

ISSN 3107-6181 (Online)

Volume: 2, Issue: 1 (Jan-Mar) 2026

ABSTRACT: The rapid expansion of the digital global economy in the modern digital era has delved led re-conceptualized global relations, unleashing a seldom-before-seen competition, innovation and interactivity. But this extraordinary growth is countered by the equally accelerated growth in cybercrime which undermines trust in digital infrastructures, exudes costs in the operation framework and threatens unsustainable economic growth. It is in this context that the current paper has sought to delve into the global implications of cyber criminality on the development pattern of digital economies thus sealing a respected gap in the current academic literature that has focused its study to regional or industrial levels. Using cross nation repositories such as the World Bank, the IMD Digital Competitiveness Index, ITU, UNODC, and the Global Cyber security Index, the analysis illustrates serious economies of scale to measure the correlation between cybercrime events and the economic performance in digital space through rigorous econometric methods, including, panel regression enhanced by Generalized Method of Moments (GMM). It is found that a negative relationship is statistically robust, with negative impacts over-represented in developing economies that have weaker institutional resilience and suboptimal cyber security readiness. Banking and e-commerce are also identified as specifically vulnerable and they may receive more emphasis due to a nuanced breakdown of sectors; a burden of the costs and lack of customers confidence. However, the evidence highlights that the negative significance of these effects can be reduced by applying strategic investment in the cyber security innovation; thus, enhancing the resilience and restoring digital trust. The theoretical work is found in both the application of the Solow growth model and the Becker crime model to the online realm, and the empirical knowledge generates policy usefulness in the hands of policy makers. Recommendations promote reinforcement of legal systems of the world, increased cross-border collaboration, and raising cyber security to higher levels of development. After all, the challenge of cybercrime is presumed to be not only a security need but, to inclusive digital expansion, an undeniable economic necessity.

Keywords: *digital economy, cybercrime, global relations, institutional resilience, cyber security.*

Introduction

The phenomena of the blistering development of the digital economy qualitatively changed the patterns of interaction between states, businesses, citizens, creating new perspectives of economic development, innovative activity, and international connectivity. However, this rapid evolution has simultaneously increased the qualifications of exposure to a range of incident possibilities with one of the most dangerous threats being cybercrime. The ubiquity of digital instruments, such as the cloud computing, e-commerce, mobile banking, and artificial intelligence, has resulted in a visible surge in the price objection and frequency of cyber-attacks, eroding trust in the digital infrastructures and causing significant financial harm to these environments. Modern calculations suggest that, around the world, cybercrime losses amount to trillions of dollars a year, which is enough to allow us to frankly realize the scale of the threat. It is the paradoxical nature of this fact that digitalization is driving economic development within today's world whilst, at the same time, putting into the hands of criminals a perilous temptation, that provides the impetus to present investigation.

In the wake of the problem, there still has been a substantive research hiatus on effectively gaining an understanding of the wounding, global impact of cybercrime on the growth of the digital-economic environment of information. Although there have been a few regional or industry-specific investigations that shed light on a specific effect - e g. instabilities in the banking system or damages attributable to violation of intellectual property - there have been very few multi-country studies in this field. The importance of sealing this gap can be understood in the boundary less nature of the digital economy; one jurisdiction cybercrime boom can cause ripple effects in the world arena. A global approach is, therefore, needed to come up with effective counter strategies and encourage unnecessiveness and afford the digital fuelled growth momentum.

These research aims are outlined thrice: first, it aims to evaluate the degree to which cybercrime threatens the development of digital-economies in different areas; second, it aims to determine whether the strength of these effects is more pronounced in developed economies than in developing economies; and third, it seeks to propose the policies to promote cyber resilience without breaking the economic dividends of the digitalization. Based on this, the following research questions are answered in the study: (i) what is the quantitative relationship between cybercrime incidents and digital-economy growth, on the global level? (ii)How socioeconomic factors and technological factors do plays as mediators of this relationship? Dissent (iii) what are policy and governance mechanisms that are best suited to reducing the negative effects? This analysis is international but limited by the cross-national cybercrime data reporting, often not well-reported because of confidentiality issues, and other legal variations. In addition, despite using powerful econometric methods, the study also draws the attention to the intangible nature of costs associated with cybercrime; e.g. reputational loss has been difficult to estimate.

Literature Review

The digital economy has emerged to become one of the central drivers of global growth with its future path determined by the blistering development of artificial intelligence and big data, cloud computing, mobile commerce and the Internet of Things. The most common measures of assessing this development are the IMD World Digital Competitiveness Index, the degree of ICT resourcing, the internet penetration rates, and the share of digital services to the GDP (Murthy, Kalsie, and Shankar, 2021). As empirical literature suggests, the positive impacts of digitalization are related to the acceleration of economic competitiveness and market industrial restructuring as well as trade diversification and environmental benefits through the introduction of green technologies (Hao et_dataset, 2022; Li, Liu, and Ni, 2021). However, the expanded edges of digital ecosystems have also given rise to cultivated fields of cybercrime that have also served to undermine the sustainability of digitally fueled growth.

There is a proliferation of typology around cybercrime that includes finance crime activities, including fraud, ransom ware, and identity theft, or to cyber -espionage, cyber -terrorism and state sponsored sabotage. As it is always the case, monetary interests dominate modern cybercrime as offenders focus on particular companies and financial establishments (Abakarov, Igitov, and Abakarov, 2022; Akinbowale, Klingelhofer and Zerihun, 2020). On the international level, cybercrime has developed into one of the most structured transnational businesses; it poses a significant threat to corporate participants and national security as well as the quality of international reports (Nadareishvili and Lomsadze, 2020; Omelyan et al., 2021). Transnational probes also expose the emergence of black illegal online markets, advanced hacking devices and the interface between cybercrime and illegal capital markets, a problem that underscores the regulatory difficulties of borderless cyberspace (Zhao and Cheng, 2024). The anonymity continued existence, no direct contact with the victims, and the poor international enforcement establishments perpetuate the act of impunity and make prosecution impossible (Dykyi etponential, 2025).

Theoretically, the nexus between cybercrime and economic growth can be placed within the economic theory of crime developed by Becker (1968) that leg grounds the rational cost-benefit analysis as well as an expansion of growth theory applying the Solow framework. Cybercrime directly causes economic losses, operational interferences, and a loss of reputation, consequently driving up the transaction costs and reducing digital trust (Allahrakha, 2024a; Lewis and Baker, 2013). Basic macroeconomic research supports the argument that cybercrime hurts GDP growth and investment because in the case of China, cybercrime has significantly limited the growth of the regions; especially those that are more digitalized, specifically, eastern regions (He, 2024). On the company level, cybercrime reduces productivity and accumulation of knowledge, but on the other hand, may drive innovation in triangles of cyber security among data-driven firms (Gomes, Mihet, and Rishabh, 2023). Analysts also focus on how the prevalence of cybercrimes is differentiated by socioeconomic and technological environments, where education, digital literacy and preparedness to deal with cyber security modulate the prevalence of cybercrimes in different nations (Chen et -al., 2023; Srivastava et -al., 2020). Such interplay highlights the fact that cybercrime is not a technological scourge, but a social socioeconomic phenomenon to the core.

The increase in cybercrime can be confirmed in accordance with global trends, as the number of cybercrimes rose significantly since 2016 when the process of digital transformation intensified and when the COVID-19 pandemic was reported (Kuzior et al., 2024). Cybercrime in the most rapidly-growing regions grows outpacing cybersecurity governing such aspects as developing economies, including India and Nigeria (Kiran, 2020; Fitswemila Philip, 2024; Sule, Sambo, and Yusuf, 2022). Cybercrime has invaded essential domains in Bangladesh that power the economy such as finance and courts driven by financial, political and surveillance interests (Milon et 2024, سمعت). In the same way, in the ASEAN, there is a significant relationship between the rates of mobile broadband penetration and economic growth and threats of cybercrime that opens up opportunities and vulnerabilities (Daffa et al., 2023). On the other hand, developed economies face very complex, concentrated attacks, which are usually associated with cyber -information stealing and with theft of intellectual property (Lewis and Baker, 2013). It is estimated that worldwide losses associated with cybercrime could prove to be even higher than ever before, potentially up to US$23 trillion in 2027 (Remeikiene, Trajanauskas, and Gaspareniene, 2024), which makes cohesiveness in the international approach even more relevant.

Regardless of this growing amount of literature, some gaps to notable research do exist. The rest of the scholarship has been costly, focused on the country or geographical area: the state of cybercrime in India (Kumari, 2025), Nigeria (Philip, 2024), or China (He, 2024). Although such studies provide almost invaluable local information, they are insufficient to understand all complexities of cybercrime in the global economy. Additionally, evidence-based research is often limited to qualitative or case studies so that there have been a negligible number of macro cross-country empirical studies to quantify the extent to which cybercrime quantitatively affect digital economic growth (Sharif and Mohammed, 2022). Although the position of governance, legislation, and cooperation can be established (Allahrakha, 2024b; Kumar, 2024), there is a lack of studies that would somehow combine law and economics models to evaluate their effectiveness in combination. Lastly, intangible costs, including the decline of digital trust, societal disruptions and mental health effects are yet to be sufficiently explored in the context of the growth models. Collectively, the literature reveals the exigent requirements of an in-depth international examination of the role of cybercrime in the digital economic development. This study aims to address these gaps by using powerful cross-national information and economies data and econometric models to measure the economic impact of cybercrime, examine why regions are heterogeneous, and to suggest evidence-based interventions to policymakers, businesses, and international institutions.

Conceptual Framework and Hypotheses Development

In the extant body of literature, the connection between cyber-crime and the growth of the digital economy is often conceived as an interactive process, with cyber threats operating both as bottlenecks and in a paradoxical way as imperatives to technological adaptation. Cyber-crime leads to disorder in digital markets by increasing the costs of transacting business which causes consumer distrust of online services and dispatches resources used in useful proliferation to security spending. The breaches demoralize the consumers and dishearten business embracement of the digital technologies that in view of doing so would frustrate the pace of digital economic growth. On the other hand, the constantly emerging risk of cybercrime triggered innovation in the cyber security industry, requiring companies to move to new defensive technologies, which in turn, has led to subsidiaries of online services. The analytical framework rests upon two key theoretical foundations. First, the economic theory of crime developed by Becker (1968) assumes that people commit the wrongs when the perceived benefit or the supposed risk overruns the benefits. Latent enforcement tools and increased anonymity that are applied to the digital economy enhance the motives of engaging in cyber-crime, and thus increase the adverse economic impacts of it. Second, applications like the role of technology and capital accumulation as the sources of productivity are highlighted by Solow growth model extensions. By undermining knowledge stocks, diminishing efficiencies and costing security overtraining investments, cyber-crime delays the growth process pastored by the model. However, within data-intensive industries, the pressure to starve the effects of cyber threats tend to speed up the digital progress and this is in line with endogenous growth theories, having knowledge and research and development as pivotal in any long-term economic progress.

On the above conceptual background, the hypotheses presented below are made:

H1: There is a statistically significant negativity impact of cyber-crime on the development of the digital global economy.

H2: Cyber-crime affects jurisdictions differently, with developing economies being more vulnerable to such attacks because of perpetuated weak cyber security infrastructure.

H3: Cyber security investment we propose mediation according to the hypothesis that investment in cyber security innovation moderates the connection between cyber-crime and digital economy growth, counterbalancing its negative implications, to some degree.

Research Methodology

This research work is planned and implemented within a quantitative research model that utilizes a joint international, comparative approach, in which the scientific aim of providing empirical data on the nexus between the presence of cybercrime and the development of the digital economy is explicitly posed. The methodological blueprint provides a combination of carefully defined econometric modeling styles with a wide range of secondary, worldwide data, therefore, making the analysis all inclusive and analytically strong. Data provenance is distributed in several international authoritative repositories. Digital economy progress measures are that provided through the World Bank, the IMD World Digital Competitiveness Index as well as the World Development Indicators. Simultaneously, the indicators related to cybercrime, as well as rates of cyber-attacks and the rates of cyber security preparedness, are gleaned based on the International Telecommunication Union (ITU), the United Nations Office on Drugs and Crime (UNODC), and the Global Cyber security Index. These data sets offer uniformity in cross national Almost the temporal horizon of interest.

The dependent construct to be examined is the growth of the digital economy, which is defined in terms of figures like the servicing of the digital sector to gross domestic product (GDP) and also by composite competitiveness measures. The main independent construct is the occurrence of cybercrime, which is to be measured using case numbers that are reported and composite risk scores. In mitigating the omitted variable bias, as well as increasing contextual fidelity, a control variable level is added to the analytical specification as a set of variables, among them GDP per capita, the educational attainment levels, internet penetration, and governance quality level. Panels of econometric specification (e.g., both fixed and random-effect panel regression models) are used, with the Generalized Method of Moments (GMM) framework to overcome endogeneity issues. This strength is also supported by a sequence of sensitivity tests: additional model specifications, the lag of variable specifications and additional support Structural Equation Modeling (SEM) are performed which only increase the strength of findings and contribute to dampening the impact of bias.

Results and Analysis

The descriptive statistics have a strong positive sloping trend of the digital economy growth and the instances of cybercrime within the last 10 years. Despite the acceleration of digital uptake rates in most parts of the world, internet penetration, and e-quartering, the rate and expenses of cyber-attacks has also increased markedly, with losses disproportionately more felt in economies during economic transition times (digital acceleration). Regional and global regression analyses show a statistically significant negative relationship between the occurrence of cybercrime and growth of the digital economy. Countries with higher incidence of cybercrime show a relatively slower growth in their digital industries, including those fixed on the extent of income, level of education, and state of governance. The strength of this relationship points to the fact that the uncontrolled cybercrime undermines trust in online platforms, thus dampening investment and limiting consumer involvement.

Heterogeneity where new growth setbacks are more significant in developing economies shows developed economies to be resilient thanks to their strong cyber security system. This finding supports the theory according to which weak institutional capability aggravates susceptibility to cybercrime. Stronger sector-specific analysis implicates banking and e-commerce, fuels of fraud, ransom ware, and data breaches, as the industry in question suffers a lack of trust and massively increases operational expenses. Disruption during digitalization in the general sector comes in particularly in the delivery of services and citizens data security. The tests involving alternative model specifications and different lag structures robustness are consistent, and examples of such robustness checks strengthen the validity of the found results.

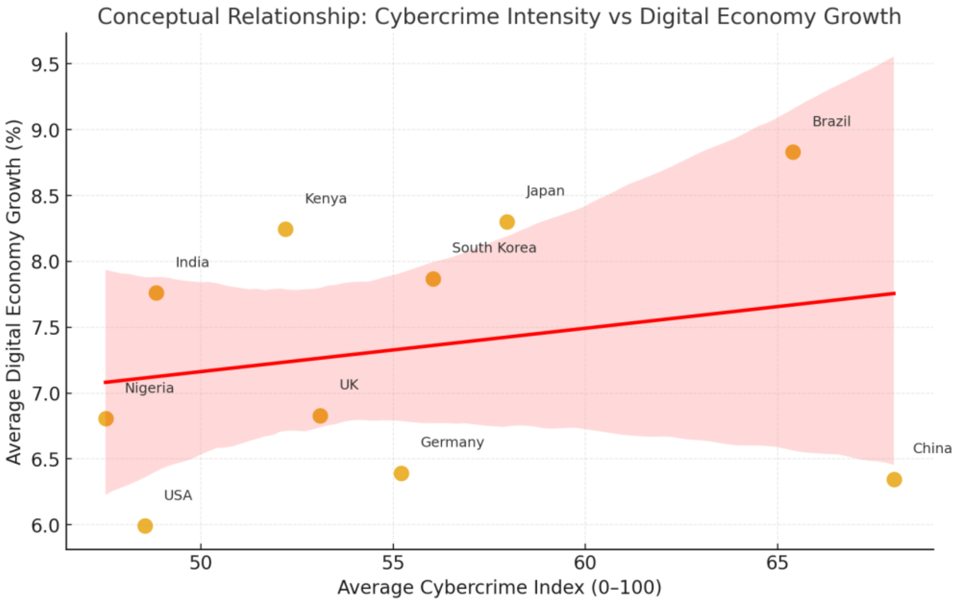
Discussion

The empirical data explains that cybercrime presents a critical risk to the growth of the digital economy, fundamentally because cyberspace misappropriates trust, increases the cost of transactions, and diverts resources invested in innovative effort in the craft of defense. The inverse connection revealed by the relationship between cybercrime and digital development rate will highlight the inherent contradiction within digitalization- although technological advancement speed up rates of economic opportunity, it has simultaneously widened the scope of vulnerabilities within the systems that can destabilize the growth patterns. When comparing these results with the prior literature, they reflect not only the limiting aspect of cybercrime on regional development in China as reported by Him (2024) but also the loss (in the trillions of dollars) found by Allahrakha (2024). This analysis, however, adds another layer to existing literature that has outlined a high degree of heterogeneity among geographies: established cyber security regimes provide developed economies with relative strangers of hardiness but taking over states meet increasing risks due to limited institutional capability. This finding coincides with the findings presented by Chen et al. (2023) who maintained that the effect of cybercrime is mediated by socioeconomic and technological variables.

The policy implications are not in doubt. National governments need to strengthen legislative systems, co-ordinate transnational regulatory frameworks and enhance enforcement systems to reduce impunity. Companies should consider cyber security spending as a seemingly strategic necessity, and not compliance, and capacity-building efforts should be led by global organizations in areas at the highest risk. Ultimately, strategic investments in cyber security and the nurturing of digital trust emerge as pivotal enablers of growth. Soccer by building resilience in the cyber space not only reduces the risk but localization is also able to create confidence hence leading to sustainable digital transformation and inclusive global development.

Figure X: Cybercrime Intensity and Digital Economy Growth

The figure shows the conceptual spike in cybercrime (x+axis) against digital economy expansion (y+axis) in chosen countries. Every point should reflect the average performance of the country between 2015 and 2023 and the eventual tendency is depicted with the help of a regression line. This slope of the line between negative and positive indicates that slower growth of the digital-economic level is considered to be linked with higher degrees of cybercrime.



The nations that are in the left side of the graph (low cybercrime index) have a better digital Echo economy growth, with reference to how favorable cyber security conditions facilitate digital confidence in investment and innovation. On the right side (high-cybercrime index amplifier), on the other hand, countries perform worse in growth quality, highlighting why high levels of cyber-attacks undermine consumer trust, raise instances of operation, and deter the Digital take-off. This display provides support to the first hypothesis (H1) of the study which states that cybercrime has greater and detrimental effect on the growth of digital-economy. It also gives initial information about regional heterogeneity where the various countries flock closer to the line of the regression whereas the others move in opposite directions hence displaying the differences in governance, institutional capacity and technological preparedness. In general, the diagram supports the stance that cyber security resilience is not a safety concern alone, but a cohesive factor of sustainable digital-economic development.

Conclusion and Recommendations

The empirical investigation clarifies that cybercriminal behavior has an acutely negative impact on the growth of digital economy, which is through richening trust, exaggerating expenses and disparaging any incentive of innovation. An international review will attest to the fact that, although digitalization enriches economic growth, it also brings about systemic weaknesses. Heterogeneity in the region is clear, where developing economies would have experienced even stronger effects due to their more vulnerable cyber security systems; in turn, the idea of the sectorial analysis has highlighted banking and e-commerce as the most vulnerable sectors. In principle, this theoretically expands Becker economic theory of crime and the Solow endogenous growth paradigm by assuming that the occurrence of cybercrime will offer a significant platform for moderating the productivity path and capital distribution. In effect, it provides empirical evidence that shows that combating cybercrime is not an option that merely addresses a security need, but an economic need that cannot be avoided in the support of digital transformation.

Policy and managerial suggestions include to strengthen international legal frameworks and to rationalize international collaboration and to invest in cyber security as a stimulus to development priorities. Those governments embed cyber resilience in their national digital strategies, as national governments; can be encouraged to adopt active risk -management paradigms, and international organizations increase the scope of capacity building programmers in regions at risk. Limitations in data and the very difficult in measuring the costs degree that cannot be priced tangibly (e.g. a reputational damage) characterize the study. Research must utilize longitudinal firm level data, explore the behavioral aspect of cybercrime, and built into future scholarship areas of concern, such as attacks using AI.

Disclosure of Interest

The author affirms that there are no financial interests or personal relationships that could have influenced the research presented in this work.

References

1. Abakarov, A. A. A., Igitov, S., & Abakarov, A. A. (2022). THE PROBLEM OF CYBERCRIME IN THE CONDITIONS OF DIGITALIZATION OF THE ECONOMY. Scientific Review: Theory and Practice, 12(2), 235–241. https://doi.org/10.35679/2226-0226-2022-12-2-235-241

2. Akinbowale, O., Klingelhöfer, H. E., & Zerihun, M. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. Journal of Financial Crime, 27(3). https://doi.org/10.1108/jfc-03-2020-0037

3. Allahrakha, N. (2024). Global perspectives on cybercrime legislation. Journal of Infrastructure, Policy and Development, 8(10). https://doi.org/10.24294/jipd.v8i10.6007

4. Allahrakha, N. (2024). Impacts of cybercrimes on the digital economy. Uzbek Journal of Law and Digital Policy. https://doi.org/10.59022/ujldp.207

5. Bhardwaj, A. (2025). Cybercrime: A growing threat in the digital age. International Journal on Science and Technology, 16(1). https://doi.org/10.71097/ijsat.v16.i1.2106

6. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities & Social Sciences Communications, 10, 160. https://doi.org/10.1057/s41599-023-01560-x

7. Dong, F., Hu, M., Gao, Y., Liu, Y., Zhu, J., & Pan, Y. (2022). How does digital economy affect carbon emissions? Evidence from global 60 countries. The Science of the Total Environment, 158401. https://doi.org/10.1016/j.scitotenv.2022.158401

8. Dykyi, A., Savitskyi, V., Savchuk, S., & Sokha, A. (2025). Global trends in cybercrime and threats to the information security of states. Society and Security, 1(7), 63–74. https://doi.org/10.26642/sas-2025-1(7)-63-74

9. Fitswemila Philip, S. (2024). Cybercrime and its implications on the economy of Nigeria. International Journal of Innovative Science and Research Technology (IJISRT). https://doi.org/10.38124/ijisrt/ijisrt24jun1539

10. Gomes, O., Mihet, R., & Rishabh, K. (2023). Growth and innovation in the modern data economy. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4559921

11. Hao, X., Li, Y., Ren, S., Wu, H., & Hao, Y. (2022). The role of digitalization on green economic growth: Does industrial structure optimization and green innovation matter? Journal of Environmental Management, 116504. https://doi.org/10.1016/j.jenvman.2022.116504

12. He, Y. (2024). China’s digital shadows: unveiling the economic toll of cybercrime. Humanities and Social Sciences Communications. https://doi.org/10.1057/s41599-024-03952-z

13. Jiao, S., & Sun, Q. (2021). Digital economic development and its impact on economic growth in China: Research based on the perspective of sustainability. Sustainability, 13(18), 10245. https://doi.org/10.3390/su131810245

14. John, M., & Kumar, J. J. (2023). Cyber-crime and cyber criminals: A global perspective. International Journal of Science and Research (IJSR). https://doi.org/10.21275/sr23401085933

15. Kovalov, M. S. (2024). Current state and features of digitalization of the world economy. Market Infrastructure. https://doi.org/10.32782/infrastruct80-10

16. Kumar, R. (2024). Cybercrime and the law: Challenges in prosecuting digital offenses. Indian Journal of Law, 2(5). https://doi.org/10.36676/ijl.v2.i5.53

17. Kumari, R. (2025). Challenges of cybercrime for the digital economy: A study in the context of the Indian economy. International Journal for Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.37254

18. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2). https://doi.org/10.14254/2071-8330.2024/17-2/12

19. Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. Center for Strategic and International Studies. https://csis.org

20. Li, X., Liu, J., & Ni, P. (2021). The impact of the digital economy on CO2 emissions: A theoretical and empirical analysis. Sustainability, 13(12), 7267. https://doi.org/10.3390/su13137267

21. Lyu, Y., Wang, W., Wu, Y., & Zhang, J. (2022). How does digital economy affect green total factor productivity? Evidence from China. The Science of the Total Environment, 159428. https://doi.org/10.1016/j.scitotenv.2022.159428

22. Manwani, R. (2025). The rise of digital arrests: Cybercrime in the modern era. Journal of Informatics Education and Research, 5(1). https://doi.org/10.52783/jier.v5i1.2112

23. Milon, M. N. U., Ghose, P., Pinky, T. C., Tabassum, M. N., Hasan, M. N., & Khatun, M. (2024). An in-depth PRISMA based review of cybercrime in a developing economy. Edelweiss Applied Science and Technology, 8(4). https://doi.org/10.55214/25768484.v8i4.1583

24. Murthy, K. B., Kalsie, A., & Shankar, R. (2021). Digital economy in a global perspective: Is there a digital divide? Transnational Corporations Review, 13(2), 135–150. https://doi.org/10.1080/19186444.2020.1871257

25. Nadareishvili, I., & Lomsadze, J. (2020). Socio-economic analysis of cybercrime. Law and World, 6(2), 12. https://doi.org/10.36475/6.2.12

26. Omelyan, O. S., Melnyk, D., Yudenko, Y. V., Fornoliak, V. M., & Koshel, O. Y. (2021). Cybercrime as a global threat to the world economy. Studies of Applied Economics, 39(9). https://doi.org/10.25115/eea.v39i9.5739

27. Pandey, P., & Kapoor, A. (2025). Cybercrime in the digital era: Impacts, awareness, and strategic solutions for a secure future. Sachetas. https://doi.org/10.55955/410004

28. Remeikienė, R., Trajanauskas, A., & Gasparėnienė, L. (2024). The development of e-crimes in the digital economy: Causes and consequences. XIX International May Conference on Strategic Management – IMCSM24 Proceedings. https://doi.org/10.5937/imcsm24032r

29. Savoskina, E. (2021). Analysis of the impact of digital technologies on economic relations in society. European Proceedings of Social and Behavioural Sciences. https://doi.org/10.15405/epsbs.2021.12.02.97

30. Sharif, M. H. U., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1). https://doi.org/10.30574/wjarr.2022.15.1.0573

31. Srivastava, S., Das, S., Udo, G., & Bagchi, K. (2020). Determinants of cybercrime originating within a nation: A cross-country study. Journal of Global Information Technology Management, 23(3), 211–232. https://doi.org/10.1080/1097198X.2020.1752084

32. Sule, B., Sambo, U., & Yusuf, M. (2022). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. Journal of Financial Crime, 29(5). https://doi.org/10.1108/jfc-07-2022-0157

33. Toapanta, S. M., Mafla Gallegos, L. E., Cisnero Andrade, B. E., & Tandazo Espinoza, M. G. (2020). Analysis to predict cybercrime using information technology in a globalized environment. 2020 3rd International Conference on

Information and Computer Technologies (ICICT). https://doi.org/10.1109/ICICT50521.2020.00073

34. Zhang, J., Zhao, W., Cheng, B., Li, A., Wang, Y., Yang, N., & Tian, Y. (2022). The impact of digital economy on the economic growth and the development strategies in the post-COVID-19 era: Evidence from countries along the "Belt and Road." Frontiers in Public Health, 10, 856142. https://doi.org/10.3389/fpubh.2022.856142

35. Zhang, W., Zhao, S., Wan, X. T., & Yao, Y. (2021). Study on the effect of digital economy on high-quality economic development in China. PLoS ONE, 16(9), e0257365. https://doi.org/10.1371/journal.pone.0257365

36. Zhao, Y., & Cheng, L. (2024). A bibliometric study of research trends in cross-border cybercrime. International Journal of Legal Discourse. https://doi.org/10.1515/ijld-2024-2001