African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Evaluation et prévision des coûts économique des risques de cybersécurité à l'aide de l'intelligence artificielle (ANALYSE EN DONNE DE PANEL)

Evaluation and Forecasting of the Economic Costs of Cybersecurity Risks Using Artificial intelligence (Panel Data Analysis).

Auteur 1 : BOUHBOUCH Mohammed-Amine.

Mohammed-Amine Bouhbouch
Economist Researcher (Holder of a Postgraduate Degree in Economics and Public Policy Evaluation from Mohamed V University, Rabat Agdal, Morocco)
Doctoral Researcher / DBA Student
EPF Engineering School, Paris, France

Déclaration de divulgation : L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.

Conflit d'intérêts : L'auteur ne signale aucun conflit d'intérêts.

Pour citer cet article : Mohammed-Amine Bouhbouch (2025) « Evaluation et prévision des coûts économique des risques de cybersécurité à l'aide de l'intelligence artificielle (ANALYSE EN DONNE DE PANEL) », African Scientific Journal « Volume 03, Num 33 » Pp: 1399 – 1421.

DOI : 10.5281/zenodo.18109868

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Résumé

La numérisation rapide des sociétés, combinée à la multiplication et à la sophistication croissante des cyberincidents, renforce la nécessité de prioriser la cybersécurité dans les stratégies d'investissement des acteurs économiques. Un défi majeur demeure toutefois : l'absence de clarté concernant les retombées économiques des investissements en cybersécurité et la compréhension limitée de l'impact réel des cyberincidents sur la performance économique. Cette étude synthétise les résultats empiriques relatifs aux économiques directs et indirects des cyberincidents et souligne les limites méthodologiques des approches d'évaluation du risque. À partir de données de panel couvrant 10 pays sur la période 2005-2024 (200 observations), L'analyse mobilise les Moindres Carrés Ordinaires (MCO), les effets fixes et l'approche par variables instrumentales (VI) afin d'estimer l'impact économiques des cyberincidents. Les résultats révèlent une forte hétérogénéité des coûts et des estimations souvent imprécises en particulier pour les effets indirects tels que les pertes de productivité et les atteintes à la réputation. La conclusion principale est que la protection efficace du cyberespace nécessite une estimation exhaustive et rigoureuse de l'ensemble des coûts économiques des cyberincidents, ce qui peut être amélioré grâce à des modèles prédictifs fondés sur l'intelligence artificielle et une collecte de données systématique.

Mots clés : incidents de cybersécurité, pertes économiques, IA, coûts directs, coûts indirects

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Abstract

The rapide digitalization of societies, coupled with the increasing frequency and sophistication of cyber incidents, has amplified the need for prioritizing cybersecurity in the investment agendas of economics actors, particularly governments and firms. However, a major challenge in mainstreaming cybersecurity investments lies in the unclear returns and the poorly understood link between cyber incidents and economic performance. This literature survey synthesizes empirical studies on both the direct and indirect costs of cyber incidents, highlighting methodological issues in risk-based approaches that could lead to misinformed decision-making. Using panel data covering 10 countries, over the period 2005-2024, totaling 200 observations, this study applies econometric evaluation techniques such as Ordinary least squares (OLS), Fixed effects (FE), and instrumental variables (IV) approaches to assess the economic impact of cyber incidents. First, it identifies the wide variation and often unfounded estimates of the economic costs, including significant indirect effects. The study concludes that accurately protecting cyberspace requires policymakers and stakeholders to understand the comprehensive economic costs of cyber incidents, which can be achieved through targeted research and systematic data collection efforts. The study concludes that effectively protecting cyberspace requires policymakers and stakeholders to gain a comprehensive understanding of the full economic costs associated with cyber incidents, which can be achieved through AI-based predictive models and systematic data collection efforts.

Keywords: Cybersecurity incidents, economic loss, defense, IA, direct costs, indirect costs.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Introduction

La transformation numérique a bouleversé les économies mondiales au cours des deux dernières décennies. L'accélération de l'utilisation des technologies de l'information et de la communication (TIC), combinée à la généralisation d'internet, a ouvert des opportunités considérables en matière de croissance, de productivité et d'innovation. Cependant, cette dépense accrue au numérique s'accompagne d'une exposition croissante aux risques de cybersécurité. Les cyberattaque, qu'il s'agisse de rançongiciels, de piratages de données, de fraudes électroniques ou de sabotages, engendrent des coûts économiques de plus en plus lourds. Selon (McAfee, 2021)[1], le coût mondial de la cybercriminalité dépasserait 1000 milliards de dollars par an, soit plus de 1% du PIB mondial. Face à ce constat, les économistes et décideurs publics cherchent à quantifier et anticiper l'impact des risques cyber sur les économies nationales. Or, cette tâche est complexe, car les données disponibles sont souvent fragmentées et les effets économiques s'expriment tant au niveau micro (entreprises, ménages) que macro (PIB, productivité, compétitivité). L'économétrie et l'intelligence artificielle offrent ici des outils puissants pour analyser et prédire ces coûts.

Ce travail propose une évaluation empirique des coûts économiques liés aux cyberattaque dans dix pays représentatifs, répartis entre économies avancées et émergentes, sur la période 2005-2024 l'utilisation de la méthode des moindres carrés ordinaires (OLS) appliquée à des données de panel permet d'identifier les facteurs explicatifs et de mesurer leur poids relatif. L'originalité de l'étude tient à l'articulation entre une approche économétrique classique et une perspective comparative internationale. La problématique qui guide cette recherche est la suivante : **Quels sont les déterminants économiques et institutionnels des coûts liés aux risques cyber et comment ces coûts évoluent-ils dans le temps et entre pays ?**

Les résultats attendus devraient permettre d'apporter un éclairage nouveau sur la manière dont les politiques publiques et les investissements privés et la résilience des pays face à ces menaces.

[1] McAfee,(2021). The hidden costs of cybercrime. McAfee Enterprise &Centre for Strategic and International Studies (CSIS). https://www.mcafee.com

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

1. Cybersécurité et coûts économiques : contexte, problématique et cadre conceptuel

1.1. Revue littérature :

1.1.1. Contexte :

La numérisation rapide des sociétés et des économies a transformé la manière dont les entreprises, les gouvernements et les citoyens interagissent. Cette transformation offre de nombreux avantages en termes d'efficacité, de productivité et d'innovation, mais elle expose couteux. Les cyberincidents, tels que les violations de données, les attaques par ransomware ou les perturbations des infrastructures critiques, peuvent générer des pertes économiques significatives, affectant la production, les revenus, la confiance des consommateurs et l'innovation technologique. La croissance exponentielle du volume des données et la dépendance accrue aux systèmes numériques rendent les économies modernes particulièrement vulnérables. Selon (l'ENISA, 2021)[2] et (Anderson et al., 2019)[3], les pertes économiques totales liées aux cyberincidents incluent à la fois les coûts directs, tels que les réparations, les amendes et les pertes immédiates de revenus, et les coûts indirects, comme la perte de productivité, l'atteinte à la réputation et l'impact sur l'investissement futur. Ces couts indirects sont souvent sous estimés ou difficiles à mesurer, ce qui complique la planification stratégique et les décisions d'investissement. Malgré l'importance croissante des cyberincidents, il existe encore un déficit majeur de données fiables et une grande hétérogénéité dans les estimations des coûts économiques. Les méthodes traditionnelles basées sur des enquêtes sectorielles ou des rapports ponctuels présentent des biais et ne permettent pas de capturer l'ensemble des effets indirects. Cette incertitude constitue un frein majeur à l'investissement en cybersécurité, tant pour les entreprises que pour les gouvernements. Les décideurs économiques ont besoin d'outils faibles pour quantifier et anticiper les coûts liés aux cyberincidents afin d'allouer efficacement les ressources et de concevoir des politiques publiques adaptées. Depuis les années 2000, La littérature académique a évolué pour quantifier les coûts économiques des cyberincidents. (Anderson et al., 2013)[4] furent parmi les premiers à conceptualiser les pertes économiques directes et indirectes des cyberattaque. (Biener et al., 2015)[5] ont quantifié les impacts assurantiels des incidents cybers, soulignant les difficultés de mesure liées à l'asymétrie d'information et au sous-reporting. La montée fulgurante de la connectivité

[2] **E**NISA. (2021). ENISA Thread Landscape 2021: The year in review. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[3] **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. In R. Böhme & T. Moore (Eds), The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-030-14506-9_9

[4] **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

[5] **B**iener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158. https://doi.org/10.1057//gpp.2014.19

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

numérique a rendu la cybersécurité un pilier essentiel de la résilience économique. Le monde connaît une multiplication des incidents de sécurité aux conséquences financières croissantes : les rapports IBM Security sur le coût des violations de données en (2023,2024,2025) montrent que le coût moyen par entreprise continue d'augmente, en grande partie à cause de l'allongement du temps de détection, de la sophistication accrue des attaques (notamment via l'IA) et de l'expansion des surfaces d'attaque (IBM Security, 2023 ; IBM Security, 2024 ; IBM Security, 2025)[6]. Ces rapports constituent des références empiriques récentes qui éclairent les tendances observables sur terrain. Outre ces évolutions structurelles, la pandémie de COVID-19 a constitué un tournant majeur. La transition rapide vers le télétravail et les services en ligne a amplifié l'exposition aux menaces numériques. Les rapports montrent une augmentation sans précédent des attaques par rançongiciels et de l'hameçonnage exploitant la thématique sanitaire (Interpol, 2020 ; ENISA, 2021)[7]. Selon (IBM, 2021)[8], le coût moyen d'une violation de données a atteint un record durant cette période, en raison de l'usage accru de dispositifs personnels non sécurisés et de l'augmentation du temps de détection. la littérature académique confirme cette tendance : (Bratik et al., 2020)[9] soulignent la vulnérabilité des PME, tandis que (Chernykh et al., 2021)[10] mettent en évidence la fragilité des secteurs de la santé et de l'éducation. Enfin, (l'OCDE, 2021)[11] note que la pandémie a conduit à une hausse des investissements publics en cybersécurité, révélant la reconnaissance accrue du risque systématique.

1.1.2. Positionnement méthodologique et épistémologique

Cette étude adopte un positionnement positiviste, visant à mesurer objectivement l'impact économique des cyberincidents sur différents pays. Le choix de l'approche quantitative et économétrique est motivé par la nécessité d'obtenir des estimations faibles et comparables des coûts économiques. Le mode de raisonnement est déductif : les hypothèses sont formulées à partir de la littérature existante et testées empiriquement. Les hypothèses principales sont :

H1 : les pays à revenu élevé subissent des coûts cyber plus élevés en raison de la densité d'actifs numériques (Anderson et al., 2019).

[6] **I**BM Security. (2023, 2024, 2025). Cost of Data Breach Report 2023, 2024, 2024. IBM Security. https://www.ibm.com/security/data-breach

[7] **I**nterpol. (2020). Interpol report on cybercrime in the COVID-19 era. Interpol. https://www.interpol.int & ENISA. (2021). ENISA Thread Landscape 2021: The year in review. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[8] **I**BM Security. (2021), Cost of a Data Breach Report 2021. IBM Security. https://www.ibm.com/security/data-breach

[9] **B**ratik, A. W., Bertrand, M., Cullen, Z. B., Glaeser, E. L., Luca, M., & Stanton, C. T. (2020). The impact of COVID-19 on small business outcomes and expectations. Proceedings of the National Academy of sciences, 117(30), 17656-17666. https://doi.org/10.1073/pnas.2006991117

[10] **C**hernykh, L., Howell, S. T., & Mandenko, K. (2021). Pandemic-induced digitalization and cyber risks in health and education sectors. Journal of Economic Behavior & Organization, 191, 850-867. https://doi.org/10.1016/j.jebo.2021.09.022

[11] **O**ECD. (2021). The COVID-19 crisis and cyber security policy responses. OCDE Publishing. https://www.oecd.org

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

H2 : La pénétration d'internet augmente la vulnérabilité aux cyberincidents (Baryshnikov, 2018).

H3 : La qualité de la gouvernance et l'investissement technologique réduisent l'impact économique des cyberincidents (IMF, 2020 ; Biener et al., 2015).

H4 : La fréquence des incidents signalés est positivement corrélée aux pertes économiques (Romanosky, 2016).

L'économétrie joue un rôle central dans la quantification des relations entre variables macro-économiques, institutionnelles et les coûts cyber. Les méthodes économétriques classiques : OLS, effets fixes (FE) et variables instrumentales (IV), pour des interprétations causales faibles.

Intelligence artificielle prédictive : réseaux neuronaux, forêts aléatoires, gradient boosting et NLP, pour enrichir les données et détecter des patterns complexes.

Cette combinaison permet de capturer les non linéarités et interactions complexes tout en maintenant la robustesse stratégiques nécessaire à des recommandations politiques faibles (Breiman, 2001 ; IBM Security, 2023 ; World Bank, 2024). Par exemple (Baryshnikov, 2018)[12], observe que dans un échantillon de pays européens, l'intensité numérique (taux d'utilisateurs internet, pénétration TIC) accroît l'exposition aux incidents, tandis que la qualité de la gouvernance tempère l'impact. (Kopp, Kaffenberger et wilson, 2017)[13] utilisent un modèle VAR pour mettre en lumière la propagation des chocs liés aux cyberattaque à l'économie financière. (Kshetri, 2016)[14] conceptualise les cyberattaque comme des « chocs négatifs de productivité » pouvant ralentir la croissance structurelle. Certains auteurs vont jusqu'à modéliser des dynamiques dans un cadre DSGE, simulant les effets macroéconomiques des cyberchocs (IMF, 2020)[15]. Plus récemment, l'intégration des méthodes de machine learning et intelligence artificielle a enrichi les capacités prédictives. (Nguyen et Kim, 2020)[16] appliquent des réseaux neuronaux pour anticiper les coûts d'attaques DDoS aux Etats-Unis. (Shaukat et al., 2020)[17] comparent la performance de l'ensemble des algorithmes (forêts aléatoire, gradient boosting, SVM) pour prédire les pertes économiques liées aux cyberincidents dans des échantillons sectoriels. Par ailleurs, (Mirsky et Shabtai, 2021)[18] exploitent le traitement du langage naturel (NLP) pour analyser les rapports de

[12] **B**aryshnikov, Y. (2018). Cyber risk insurance: A market solution to a market problem. Journal of Risk and Insurance, 85(4), 967-988. https://doi.org/10.1111/jori.12227

[13] **K**opp, E., Kaffenberger, L., & Wilson, C. (2017).Cyber risk, market failures, and financial stability. Journal of Financial Stability, 34, 52-60. https://doi.org/10.1016/j.jfs.2017.03.001

[14] **K**shetri, N. (2016). Cybersecurity and international relations. Third World Quarterly, 37(5), 832-853. https://doi.org/10.1080/01436597.2015.1116363

[15] **I**MF. (2020).The macroeconomics of cyber risk: shocks and resilience. International Monetary Fund. https://www.imf.org

[16] **N**guyen, T., & Kim, H. (2020). Predicting the economic impact of DDoS attacks with neural networks. Journal of Information Security and Applications, 54, 102556. https://doi.org/10.1016/j.jisa.2020.102556

[17] **S**haukat, K., Luo, S., Varadharaajan, V., Hameed, I.A., & Xu, M. (2020). Cyber threat detection using machine learning: Comparative analysis. Computers & Security, 99, 102104. https://doi.org/10.116:j.cose.2020.102104

[18] **M**irsky, Y., & Shabtai, A. (2021). Deep learning for cyber security: Challenges and opportunities. IEEE Transactions on Dependable and Secure Computing, 18(2), 982-995. https://doi.org/10.1109/TDSC.2020.2973659

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

sécurité, les dépôts réglementaires et extraire des signaux cachés de pertes potentielles. L'utilisation du NLP facilite l'enrichissement des bases de données avec des indicateurs textuels supplémentaires. L'apport des ces méthodes hybrides est double : d'une part, elles capturent les non-linéarités, interactions complexes, effets de seuil et hétérogénéités qui échappent aux modèles linéaires ; d'autre part, les modèles économétriques permettent une interprétation causale claire, essentielle pour la formulation de recommandations politiques (Breiman, 2001)[19]. De nombreuses études récentes insistent sur cette complémentarité : on utilise l'IA pour prédire et détecter, et l'économétrie pour expliquer et conseiller (IBM Security, 2023 ; World Bank, 2024 ; ENISA, 2023)[20]. La littérature empirique identifie plusieurs facteurs explicatifs robustes. Le revenu par habitant (PIB par habitant) est fréquemment corrélé positivement aux coûts absolus des incidents, car les pays à revenu élevé possèdent un parc d'actifs numériques dense (Anderson et al., 2019)[21].Le taux de pénétration d'internet est un vecteur de vulnérabilité directe : plus une population est connectée, plus les points d'entrée s'infléchissent (Baryshnikov, 2018)[22]. Inversement, les dépenses en R&D et l'indice de gouvernance exercent des effets atténuateurs : des institutions solides, des cadres réglementaires robustes, et des investissements technologiques améliorent la résilience faces aux attaques (IMF, 2020 ; Biener et al., 2015)[23]. Enfin, la fréquence des incidents signalés est corrélée positivement aux pertes, ce qui justifie son intégration comme variable directe de risque (Romanosky, 2016 ; Shaukat et al., 2020)[24]. Cependant, plusieurs limites demeurent d'abord,

- la dispersion méthodologique des études.
- disparité des mesures de coûts.
- hétérogénéité des sources.
- complique les comparaisons.

[19] **B**reiman, L. (2021). Random forests. Machine Learning, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324

[20] **I**BM Security. (2023). Cost of Data Breach Report 2023. IBM Security. https://www.ibm.com/security/data-breach & World Bank. (2024). Cybersecurity economics for emerging markets. World Bank Group. https://www.worldbank.org & ENISA. (2023). ENISA Thread Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[21] **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. In R. Böhme & T. Moore (Eds), The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-030-14506-9_9

[22] **B**aryshnikov, Y. (2018). Cyber risk insurance: A market solution to a market problem. Journal of Risk and Insurance, 85(4), 967-988. https://doi.org/10.1111/jori.12227

[23] **I**MF.(2020). The macroeconomics of cyber risk: shocks and resilience. International Monetary Fund. https://www.imf.org & **B**iener, C., Eling, M., & Wirfs, J.H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158. https://doi.org/10.1057/gpp.2014.19

[24] **S**haukat, K., Luo, S., Varadharaajan, V., Hameed, I.A., & Xu, M. (2020). Cyber threat detection using machine learning: Comparative analysis. Computers & Security, 99, 102104. https://doi.org/10.116:j.cose.2020.102104 & **R**omanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Deuxièment, la sous-déclaration est un biais persistant, surtout dans les économies émergentes où la transparence est moindre. Troisièmement, l'arrivée rapide de technologies émergentes (Cloud, IoT, IA) modifie les vecteurs et la dynamique des cyberattaque : certains rapports alertent sur des menaces nouvelles (Supply Chain, attaques pilotées par IA) qui nécessitent études restent centrées sur l'Amérique du Nord et l'Europe, laissant un vide empirique pour l'Afrique, l'Asie du sud et l'Amérique latine.

Afin de garantir la rigueur scientifique et la clarté conceptuelle, cette étude s'appuie sur un ensemble de mots-clés définis selon les standards internationaux. La cybersécurité est comprise comme la préservation de la confidentialité, de l'intégration et de la disponibilité des systèmes d'information dans le cyberespace (ISO/IEC 27032 ; NIST)[25], tandis que les cyberincidents désignent tout événement compromettant ces systèmes (ENISA). L'analyse des coûts économiques se fonde sur la distinction entre coûts directs, c'est-à-dire les pertes financières et opérationnelles immédiates (WEF, 2020)[26], et coût indirecte, incluant les pertes immatériels telle que la réputation, la confiance, l'innovation et la productivité (OCDE, 2021)[27]. L'intelligence artificielle (IA), définie par (OCDE, 2019)[28] comme un système algorithmique capable de percevoir son environnement, d'apprendre et de prendre des décisions, constitue un levier méthodologique central pour la prévision et l'évaluation économétriques des impacts des cyber-risques (wooldridge, 2019 ; United Nations Statistics Division, 2020)[29]. Par ailleurs, la notion de résilience numérique, entendue comme la capacité des organisations et des sociétés à prévenir, résister, se rétablir et s'adapter face aux perturbations numériques (Banque mondiale, 2022)[30] souligne l'importance de la gouvernance, définie par (OCDE, 2015)[31] comme l'ensemble des structures et processus permettant une régulation efficace et transparente. L'intégration de ces concepts et mots-clés dans la revue de littérature assure la solvabilité

[25] International Organization for Standardization. (2012). ISO/IEC 27032:2012-Information technology-Security techniques-Guidelines for cybersecurity. ISO. https://www.iso.org/standar/44375.html

[26] World Economics Forum. (2020). Global risks report 2020. WEF. https://www.weforum.org/reports/the-global-risks-report-2020

[27] Organisation de coopération et de développement économiques. (2021). Economic aspects of cybersecurity: The costs of (in) security. OCDE Publishing. https://doi.org/10.1787/5K420q9vwr8g-en

[28] Organisation de coopération et de développement économiques. (2019). OCDE principales on Artificial intelligence. OCDE. https://www.oecd.org/going-digital/ai/principales

[29] Wooldridge, J.M. (2019). Introductory econometrics: A modern approach (7th ed.). Cengage learning. & United Nations Statistics Division. (2020). Handbook on statistical organization: Third edition—The operation and organization of a statistical agency. United Nations. https://unstats.un.org/unsd/publication/seriesf_88e.pdf

[30] World Bank. (2022). World Development report 2022: Finance for an equitable recovery. World Bank. https://doi.org/10.1596/978-1-4648-1730-4

[31] Organisation de coopération et de développement économiques. (2015). OECD regulatory policy outlook 2015. OCDE Publishing. https://doi.org/10.1787/9789264238770-en

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

scientifique du travail et permet une analyse comparative internationale et interdisciplinaire des coûts économiques liés aux cyberincidents.

1.1.3. Cadre conceptuel de l'évaluation et de la prévision des coûts économiques des cyberincidents à l'aide de l'IA :

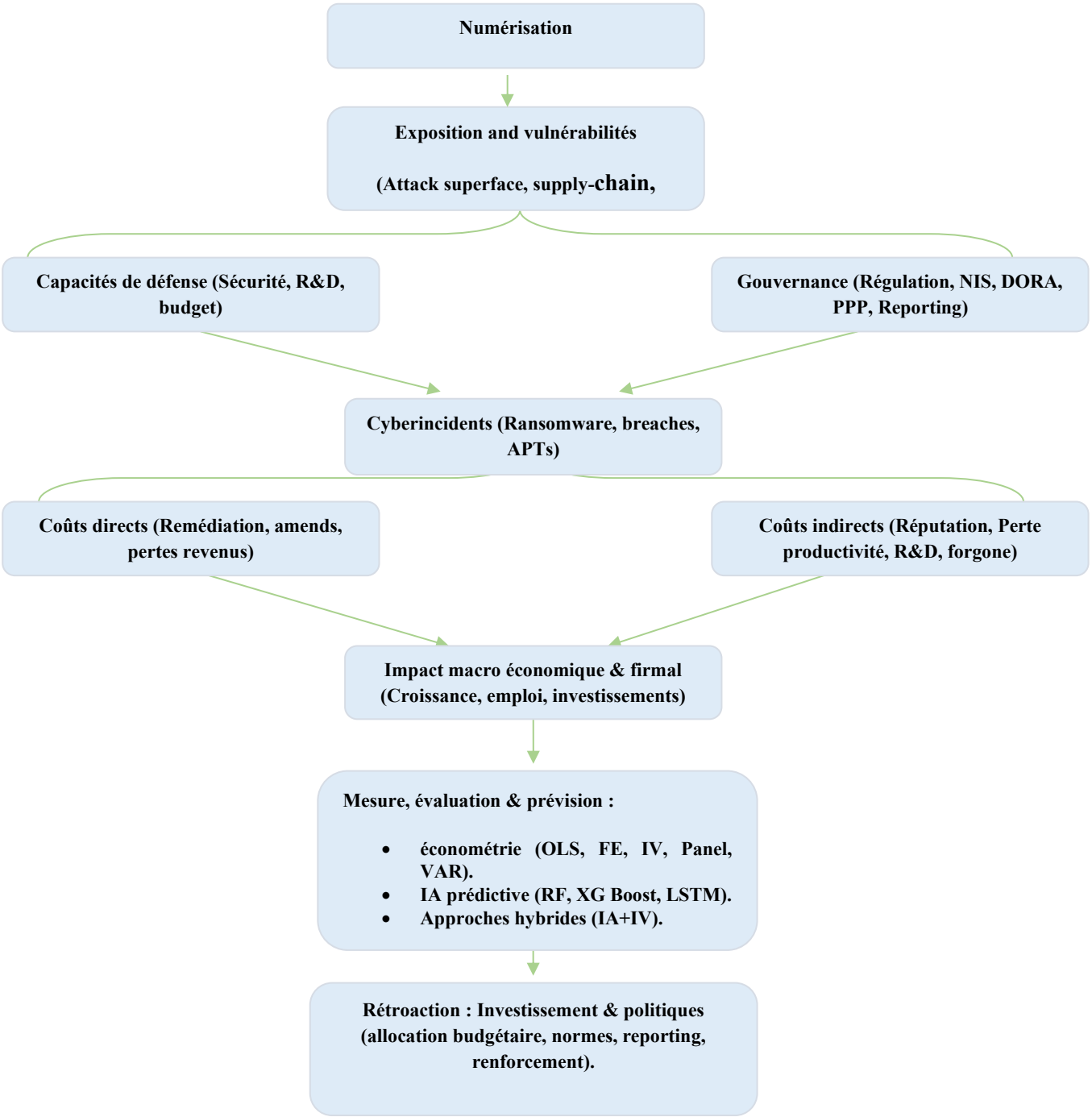

FIGURE N°1 : SCHEMA CONCEPTUEL DE L'EVALUATION ET DE LA PREVISION DES COUTS ECONOMIQUES DES CYBERINCIDENTS A L'AIDE DE L'IA

SOURCE : ETABLIR PAR AUTEUR

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Le cadre conceptuel élaboré dans cette étude propose une représentation intégrative des mécanismes par lesquels les cyberincidents affectent l'économie réelle et la gouvernance publique. Au sommet du modèle, les cyberincidents sont identifiés comme point de départ générateur de perturbations multidimensionnelles. Ces événements, qui englobent des attaques telles que les instructions, les vols de données ou les ransomware, se traduisent par deux catégories de coûts : directs, comprenant les dépenses de Remédiation, la perte immédiate de liquidités et les interruptions opérationnelles ; et indirects, couvrant des externalités plus diffuses telles que la dégradation de la réputation, l'érosion de la confiance des consommateurs et investisseurs, ou encore l'affaiblissement de la productivité et de l'innovation. L'agrégation de ces effets engendre les coûts économiques globaux, lesquels constituent l'objet central de l'analyse.

Ce processus analytique s'appuie sur une base empirique solide : un panel de dix pays et deux cents observations annuelles (2005-2024), permettant une couverture temporelle et spatiale adéquate pour identifier les tendances et divergences structurelles. Afin de dépasser les limites des approches purement descriptives, le modèle intègre une double dimension méthodologique : d'une part, des méthodes économétriques classiques. Garantissant robustesse et validité statistique ; d'autre part, l'intelligence artificielle prédictive, offrant une capacité d'anticipation et de modélisation des scénarios futurs.

L'articulation de ces deux dimensions conduit à une analyse comparative internationale, visant à mettre en lumière les convergences et divergences entre économies nationales en matière de résilience numérique. En aval, les résultats produits alimentent les politiques publiques et dispositifs de gouvernance, en fournissant aux décideurs des éléments probants pour l'élaboration de stratégies de cybersécurité fondées sur l'évidence scientifique. Enfin, l'objectif ultime de ce cadre est de contribuer au renforcement de la résilience numériques et du développement économique durable, en reliant la compréhension micro-économique des coûts aux enjeux macro-économiques de croissance et de stabilité.

1.1.4. Mise en perspective comparative :

Le cadre conceptuel proposé dans cette étude s'inscrit dans la continuité des travaux existants tout en introduisant des avancées méthodologiques majeures. En effets, Anderson et al., (2013)[32] ont ouvert la voie à une évaluation structurée des coûts de la cybercriminalité en distinguant les dimensions directes et indirectes, mais leur approche demeure essentiellement descriptive et centrée sur l'espace européen. De même, Kopp, Leigh, Luca et Wilson (2017)[33] ont souligné le

[32] **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme & T. Moore (Eds), The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

[33] Kopp, E., Leigh, A., & Wilson, C.(2017). Cyber risk, market failures, and financial stability (IMF Working Paper No. 17/185). International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2017/07Cyber-Risk-Market-Failures-and-Financial-Stability-45103

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

lien entre cyber-risque, asymétries d'information et stabilité macroéconomique, mais sans recourir à des modèles économétriques comparatifs ni à des outils de prévision avancés. Par ailleurs, les rapports du World Economic Forum (2020)[34] mettent en évidence les interdépendances globales des cybermenaces dans une perspective qualitative et prospective, mais proposent pas de cadre opérationnel d'évaluation chiffrée. En comparaison, le présent modèle conceptuel innove en intégrant, d'une part, une base de données de panels couvrant 10 pays et deux décennies (2005-2024) et, d'autre part, des méthodes économétriques enrichies par l'intelligence artificielle prédictive. Cette double articulation permet non seulement de quantifier les coûts économiques globaux des cyberincidents, mais également d'en anticiper l'évolution dans une perspective internationale et comparative. Ainsi, l'étude apporte une contribution originale à la littérature en renforçant le dialogue entre économie appliquée, cybersécurité et gouvernance publique.

1.1.5. Conclusion sur les risques de cybersécurité :

La littérature récente converge vers l'idée que la numérisation accrue des sociétés et des économies amplifie l'exposition aux risques de cybersécurité, en raison de l'augmentation des surfaces d'attaque, de la sophistication des cyberincidents et de la dépendance croissante aux systèmes numériques. Cependant, la gouvernance institutionnelle, la capacité technologique et l'investissement stratégique en cybersécurité jouent un rôle d'amortisseur essentiel, limitant l'impact économique et opérationnel des incidents. Les rapports récents d'IBM Security fournissent des points de calibration empirique incontournables, démontrant que la combinaison de données historiques et d'indicateurs sectoriels permet de mieux comprendre l'ampleur et la dynamique des risques. Par ailleurs, l'intégration de techniques d'intelligence artificielle dans une architecture économétrique offre une approche prometteuse pour évaluer et anticiper les coûts économiques des cyberincidents, en capturant les interactions complexes, les effets non linéaires et les tendances émergentes à l'échelle internationale. Ainsi, Cette convergence entre numérisation, gouvernance, capacités technologiques et outils prédictifs constitue la base pour une gestion proactive et fondée sur des preuves des risques de cybersécurité, tant pour les entreprises que pour les décideurs publics.

Dans l'analyse des coûts économiques des cyberincidents, plusieurs variables explicatives principales sont identifiées dans la littérature et justifiées par leur impact sur la vulnérabilité ou la résilience face aux risques cyber. Les incidents cybernétiques représentent la variable clé, capturant la fréquence et la gravité des attaques (Romanosky, 2016 ; Shaukat et al., 2020). Le PIB et la population sont utilisés pour mesurer la taille et la richesse économique d'un pays, influençant la densité des actifs numériques et donc l'exposition aux cybers risques (Anderson et al., 2019 ;

[34] World Economics Forum. (2020). Global risks report 2020. WEF. https://www.weforum.org/reports/the-global-risks-report-2020

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Baryshnikov, 2018). Les dépenses en R&D et les infrastructures numériques reflètent la capacité technologique et la préparation des systèmes, atténuant les effets des cyberincidents (IMF, 2020 ; Biener et al., 2015). L'indice de gouvernance permet d'évaluer l'efficacité institutionnelle et réglementaire dans la prévision et la gestion des incidents cybers (World Bank, 2024). Le commerce international est intégré comme proxy de l'exposition aux flux économiques et aux chaines d'approvisionnement, potentiellement vecteurs de cyberattaques. Enfin la variable Covid-19 capte l'effet de la pandémie sur l'accélération de la numérisation et l'augmentation des risques cyber, tandis que ln_cost (logarithme des coûts économiques) constitue la variable dépendante principale, permettant d'analyser les variations des pertes économiques dans un cadre économétrique comparatif. Cette identification des variables explicatives, basée sur des fondements empiriques solides, permet de structurer le modèle économétrique et prédictif, en cohérence avec les recommandations de la littérature internationale sur l'évaluation des risques cyber et leurs impacts économiques.

2. le cadre méthodologique d'évaluation et prévision des couts économiques des risques de Cybersécurité à l'aide de l'intelligence artificielle

2.1. Cadre méthodologique :

La solidité scientifique d'une recherche doctorale repose en grande partie sur la rigueur de ma méthodologie. Dans le cadre de cette étude, consacrée à l'évaluation et à la prévision des coûts économiques liés aux risques de cybersécurité à l'aide de l'intelligence artificielle, la méthodologie adoptée vise à articuler une approche économétrique robuste et des techniques prédictives avancées. Cette démarche sa justifie par la complexité croissante des cyberincidents, dont les impacts économiques dépassent désormais les frontières nationales et appellent à une analyse comparée entre plusieurs pays. L'élaboration du dispositif méthodologique repose sur trois piliers essentiels : la constitution d'une base de données internationale couvrant 10 pays sur une période allant de 2005 à 2024, ce qui permet d'exploiter la richesse des observations longitudinales et d'analyser les dynamiques temporelles. Ensuite, la mise en place de modèles économétriques en panel, mobilisant des méthodes telles que les (MCO), les effets fixes et aléatoires, ainsi que les tests de robustesse, afin de capter les relations structurelles entre cybersécurité, activité économique et variables institutionnelles. Enfin, l'intégration de l'IA dans la modélisation prévisionnelle, à travers des algorithmes tels que les réseaux neuronaux ou les forêts aléatoires, offre une valeur ajoutée dans la capacité à anticiper les coûts futurs des cyberattaque, en complétant les limites des approches économétriques classiques. Cette combinaison entre méthodes quantitatives traditionnelles et approches innovantes répond à un double impératif : assurer la validité scientifique de l'analyse et fournir des résultats opérationnels aux décideurs publics et privés. Ce chapitre expose donc en détail le cadre méthodologique retenu, depuis la définition

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

conceptuelle et la formulation des hypothèses jusqu'aux méthodes d'estimation et de prévisions, tout en mettant en évidence les choix stratégiques qui fondent la pertinence et la fiabilité des résultats attendus.

Données :

-Panel de 10 pays (2005-2024)

-200 observations

-Variables principale : incidents cybernétiques, PIB, population, dépenses R&D, infrastructures numériques, gouvernance, commerce international, Covid-19, ln_cost.

Modèle de base :

$$\ln(cost_{it}) = \sigma + \beta_1 \ln(RD_{it}) + \beta_2 \ln(GDP_{it}) + \beta_3 \ln(Secit_{it}) + \ldots + \varepsilon_{it}$$

2.2. Les résultats économétriques :

Tableau n°1: Linear regression

ln_cost	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
covid_19	.482	.485	0.99	.321	-.474	1.438	
ln_RD	2.53	1.023	2.47	.014	.511	4.548	**
ln_GDP	-.805	.425	-1.89	.06	-1.644	.033	*
ln_POP	1.52	.334	4.56	0	.862	2.178	***
ln_INTR	.983	.295	3.33	.001	.401	1.566	***
ln_SECUR	.022	.044	0.50	.617	-.064	.108	
ln_BROA	.146	.381	0.38	.702	-.605	.896	
ln_GOV	-.298	.596	-0.50	.617	-1.474	.877	
ln_TRAD	-.151	.577	-0.26	.793	-1.29	.987	
Constant	7.414	7.374	1.01	.316	-7.131	21.96	

Mean dependent var	19.158	SD dependent var	2.403
R-squared	0.367	Number of obs	200
F-test	12.233	Prob > F	0.000
Akaike crit. (AIC)	845.818	Bayesian crit. (BIC)	878.802

*** p<.01, ** p<.05, * p<.1

Source: établir par auteur sur application STATA

Breusch-Pagan / Cook-Weisberg test for heteroskedasticity
Ho: Constant variance
Variables: fitted values of ln_cost
chi2(1) = 2.50
Prob > chi2 = 0.1135

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Tableaux n°2: Cameron & Trivedi's decomposition of IM-test

Source	Chi2	df	P
Heteroskedasticity	109.41	53	0.0000
Skewness	34.95	9	0.0001
Kurtosis	11.92	1	0.0006
Total	156.28	63	0.0000

Source: établir par auteur sur application STATA

Tableau n°3 : Variance inflation factor

	VIF	1/VIF
ln GDP	33.273	.03
ln BROA	12.605	.079
ln POP	9.816	.102
ln GOV	8.243	.121
ln RD	7.191	.139
ln INTR	3.95	.253
ln TRAD	1.864	.536
ln SECUR	1.724	.58
Covid 19	1.104	.906
Mean VIF	8.863	.

Source: établir par auteur sur application STATA

Tableau n°4 : Instrumental variables (2SLS) regression

ln_cost	Coef.	St.Err.	t-value	p-value	[95% Conf	Interval]	Sig
ln_SECUR	.221	.109	2.04	.042	.008	.434	**
ln_TRAD	-2.097	.582	-3.60	0	-3.238	-.957	***
Constant	26.114	2.186	11.94	0	21.829	30.399	***

Mean dependent var	19.158	SD dependent var	2.403
R-squared	.	Number of obs	200
Chi-square	13.646	Prob > chi2	0.001

**** p<.01, ** p<.05, * p<.1*

Source: établir par auteur sur application STATA

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Tableau n°5: First-stage regression summary statistics

Variable	Adjusted R-sq.	Partial R-sq.	Robust R-sq.	F (1,197)	Prob > F
ln_SECUR	0.2243	0.2164	0.2100	55.9437	0.0000

Source: établir par auteur sur application STATA

2.3. Interprétations :

Le tableau de régression OLS (dépendante : ln_cost) montre que le modèle explique de manière modérée la variation des coûts liés à la cybersécurité ($R^2 = 0.3669$). Le test F global est significatif ($F(9,190)= 12.23$, $p<0.001$), indiquant que l'ensemble des variables explicatives contribue conjointement à expliquer ln_cost.

Parmi les coefficients, ln_RD (Coef=2.5298, p=0.014) apparaît fortement et positivement lié aux coûts : une augmentation propositionnelle des dépenses en R&D est associée à une hausse des coûts de cybersécurité, ce qui peut refléter (i) un effet de détection-plus de R&D expose ou identifie davantage de vulnérabilités- ou (ii) des activités de R&D plus intensives en technologies numériques qui augmentent la surface d'attaque. ln_POP (1.5202, p<0.001) et ln_INTR (0.9835, p=0.001) sont également positifs et significatifs, cohérents avec l'hypothèse que une population plus nombreuse et un usage d'internet plus élevé accroissent l'exposition et, par conséquent, les coûts agrégés (Anderson et al., 2013)[35]. En revanche, covid_19 n'est pas statistiquement significatif (0.4819, p=0.321) dans ce modèle OLS, ce qui suggère l'absence d'effet direct détectable du seul indicateur COVID sur ln_cost lorsque les autres variables sont contrôlées. Ln_GDP présente un effet négatif marginalement significatif (-0.8052, p≈0.06), pouvant indiquer qu'un niveau de développement économique plus élevé réduit l'effet doit être interprété avec prudence (cf. multicolinéarité infra).

- Test d'hétéroscédasticité (Breusch-Pagan) et diagnostic IM-test :

Le test Breusch-Pagan appliqué aux valeurs ajustées n'autorise pas de rejeter l'hypothèse d'homoscédasticité (p=0.1135). Toutefois, la décomposition de Cameron & Trivedi (IM-test)[36] révèle une combinaison significative d'hétéroscédasticité, d'asymétrie et d'excès de Kurtosis (p<0.001 au total). Cette contradiction n'est plus sensible aux déviations de la normalité et à des

[35] **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme & T. Moore (Eds), The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

[36] **C**ameron, A. C., & Trivedi, P. K. (1990). The information matrix test and its applied alternative hypotheses. Journal of Econometrics, 47(1), 115-148. https://doi.org/10.1016/0304-4076(90)90085-R

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

formes complexes d'hétéroscédasticité. Par prudence économétrique, il convient d'employer des estimateurs robustes aux erreurs hétéroscédastiques (erreurs standards robustes ou estimation par 2sls robustes) et/ou de tester des régressions sur des sous-échantillons.

- Multicolinéarité (VIF) :

Les statistiques VIF indiquent une forte multicolinéarité, en particulier pour ln_cost (VIF = 33.27) et ln_BROA (VIF = 12.61), avec une moyenne VIF≈ 8.86. Une VIF aussi élevée pour ln_GDP signale que les effets marginaux associés à cette variable sont estimés avec une grande variance : les intervalles de confiance et la signification statistique peuvent être artificiellement instables. Pour améliorer l'interprétabilité et la fiabilité des coefficients, il est recommandé de : (i) vérifier les corrélations simples entre variables, (ii) envisager de retirer ou regrouper des variables fortement corrélées (par ex : créer un indice synthétique via ACP pou l'ICT), (iii) centrer ou standardiser certains variables, ou (IV) estimer des modèles alternatifs (régressions partielles, modèles à facteurs, ou réduction de dimension).

- Estimation par variables instrumentales (2SLS)- ln_SECUR instrumentée par ln_GOV :

Etant donné un soupçon d'endogénéité pour ln_SECUR, j'ai instrumenté ln_SECUR par ln_GOV, la seconde étape (2SLS robuste) montre que ln_SECUR devient significatif et positif (Coef = 0.2210, p=0.042), contrairement à l'OLS. Ce changement indique que l'estimation OLS était probablement biaisée (par exemple par corrélation simultanée ou par erreur de mesure). L'effet positif estimé en 2SLS signifie que, toutes choses égales par ailleurs, une hausse de la variable de cybersécurité est associée à une augmentation des coûts observés ce qui peut traduire l'effet de détection et d'investissement : plus un pays/ménage/entreprise investit officiellement en cybersécurité, plus il identifie, rapporte et comptabilise des coûts (ou engage des dépenses de mitigation) à court terme. Ce résultat demande une interprétation nuancée : un coefficient significatif ne prouve pas que l'accroissement de sécurité augmente la vulnérabilité intrinsèque, mais peut refléter des dynamique signalement et d'investissement (Kopp et al., 2017)[37].

- Validité et forte de l'instrument (first stage) :

Le bilan du premier stade est satisfaisant : R-sq ajusté ≈ 0.2243, partial $R^2 \approx 0.21$ et (1.197) =55.94 ($p<0.001$), montrant un instrument fort (règle pratique : F>10). L'instrument ln_GOV explique une part non négligeable de la variation de ln_SECUR, réduisant le risque de biais par instrument faible. Reste à vérifier l'exclusion restriction : ln_GOV doit affecter ln_cost uniquement via ln_SECUR. Cette hypothèse est forte. Alors, la discussion si les dépenses publiques (ln_GOV)

[37] Kopp, E., Leigh, D., Luca, A., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund (IMF) Staff Discussion Note, SDN/17/05. https://doi.org/10.5089/9781484315224.006,

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

peuvent aussi influencer directement les coûts (par exemple via santé, formation, régulation) ; un test d'exclusion ou instruments alternatifs/ajoutés renforcerait la crédibilité.

- Interprétation économique et implications politiques :

- Effets d'exposition : la significativité de ln_POP et ln_INTR confirme que l'ampleur de la population et la pénétration d'internet sont des moteurs robustes des coûts liés aux cyber-risques.les politiques qui ciblent la réduction de la surface d'attaque (sensibilisation, segmentation des réseaux). Sont pertinentes.

- R&D : l'effet positif de ln_RD illustre un paradoxe : l'activité R&D amplifie les coûts à court terme (détection, complexité), les décideurs doivent donc coupler soutien à l'innovation et mesures de cybersécurité proactives (normes, financement de la sécurité).

- Rôle du commerce : La forte association négative de ln_TRAD en 2SLS suggère que l'ouverture commerciale peut réduire les coûts, possiblement via transfert de bonnes pratiques et diffusion technologique.

- Covid-19 : L'absence d'effet direct significatif du Covid-19 dans l'OLS invite à explorer des effets indirects ou non linéaires (ex : interaction Covid-19 × ln_INTR ou variants temporels), la pandémie a peut-être modifié les canaux (télétravail, accélération digitale), plutôt d'avoir un effet uniforme.

2.4. Conclusion sur le cadre méthodologique:

Les résultats économétriques obtenus permettent d'évaluer empiriquement la validité des hypothèses avancées dans le cadre théorique. Le modèle **OLS** révèle que les déterminants structurels des coûts cyber sont globalement cohérents avec les prédictions de la littérature, bien que certaines relations nécessitent des interprétations nuancées. La significativité positive de **ln_POP** et **ln_INTR** confirme l'hypothèse **H2**, selon laquelle une exposition numérique plus large via la croissance démographique et la pénétration d'internet intensifie mécaniquement les risques et les coûts associés. Cette dynamique corrobore les travaux (Baryshnikov, 2018) , et (Anderson et al.,2013). De même, les résultats montrent que **ln_RD** exerce un effet fortement positif sur les coûts, validant partiellement **H3** : une intensification de l'activité technologique accroît la surface d'attaque et améliore les capacités de détection, ce qui augmente les coûts enregistrés à court terme. Cependant, cet effet reflète davantage un mécanisme de détection/amélioration technique qu'une détérioration réelle de la sécurité. Concernant **ln_GDP**, le signe négatif mais faiblement significatif suggère qu'un niveau de développement économique élevé pourrait amortir les coûts, comme anticipé dans **H1**. Néanmoins, la forte multicolinéarité détectée particulièrement autour de **ln_GDP** et des variables d'infrastructure invite à interpréter ce résultat avec prudence. L'analyse par variables instrumentales apporte un éclairage décisif : une fois instrumentée par **ln_GOV**, la variable **ln_SECUR** devient positive et significative, validant ainsi **H3** sous un angle différent.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

Cette relation indique que les efforts de cybersécurité, loin de réduire mécaniquement les coûts, conduisent à un meilleur signalement et à une prise en charge accrue des incidents. Le rôle de la gouvernance apparait donc structurant, tant comme facteurs explicatif que comme instrument robuste, En cohérence avec **H4**, les modèles **OLS** et **2SLS** soutiennent l'idée que la dynamique des incidents signalés et des investissements de sécurité sa traduit par une hausse des coûts mesurés, ce qui rejoint les conclusions de (Romanosky, 2016). Enfin, l'absence de significativité de la variable **covid_19** suggère que la pandémie n'a pas produit d'effet direct isolable sur les coûts, une observation cohérente avec l'idée que ses impacts sont indirects, sectoriels ou non linéaires. Dans l'ensemble, ces résultats confirment empiriquement les hypothèses **H1**, **H2** et **H4**, tandis que **H3** est partiellement validée mais dépendante des spécifications instrumentales et du degré de multicolinéarité. Ils soulignent l'importance cruciale de l'exposition numérique, des capacités institutionnelles et des structures technologiques dans la détermination des coûts économiques liés à la cybersécurité, tout en mettant en évidence les limites des modèles **OLS** lorsque les problèmes d'endogénéité et d'instabilité des coefficients ne sont pas corrigés.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

3. Conclusion générale :

Ce travail avait pour objectif d'évaluer et de prévoir les coûts économiques associés aux risques de cybersécurité à l'aide d'une approche intégrant des méthodes économétriques en données de panel et des indicateurs dérivés de l'intelligence artificielle. En mobilisant un ensemble un ensemble des variables structurelles incidents cybernétiques, PIB, population, dépenses de R&D, infrastructures numériques, gouvernance, commerce international et Covid-19 l'étude a permis d'analyser empiriquement les déterminants des pertes économiques liées aux cyberincidents dans un échantillon international. Les résultats montrent que l'exposition numérique, mesurée par la population et la pénétration d'internet, constitue un moteur robuste de l'augmentation des coûts. Les dépenses en R&D contribuent également à accroître les coûts, un phénomène attribuable à l'intensification technologique et à l'amélioration des capacités de détection. La gouvernance apparaît comme un facteur essentiel : instrumentée dans le modèle 2SLS, elle révèle que le renforcement des dispositifs de cybersécurité améliore le signalement et la prise en charge des risques, ce qui influence directement les coûts observés. Ces conclusions confirment en grande partie les hypothèses théoriques formulées et s'inscrivent dans les tendances décrites par la littérature récente sur l'économie de la cybersécurité. Au plan méthodologique, l'étude met en évidence les limites des estimations OLS en présence d'endogénéité et de multicolinéarité. L'utilisation de variables instrumentales (2SLS) améliore la robustesse des résultats et montre la pertinence d'approches économétriques avancées pour l'analyse des risques cyber. L'intégration potentielle de techniques d'intelligence artificielle dans l'architecture économétrique ouvre également des perspectives prometteuses pour affiner les prévisions et réduire les biais liés au signalement ou aux erreurs de mesure. Cependant, ce travail comporte plusieurs limites. D'abord, la disponibilité et la qualité des données sur les incidents cybernétiques restent inégales selon les pays, ce qui peut entrainer des biais de mesure. Ensuite, la multicolinéarité observée entre certains variables structurelles, notamment entre PIB, infrastructures numériques et commerce internationale, réduit la précision de certains coefficients, De plus, l'utilisation d'un seul instrument pour corriger l'endogénéité de la cybersécurité limite la capacité à tester rigoureusement l'hypothèse d'exclusion. Enfin la variable Covid-19, peu significative dans les modèles estimés, gagnerait à être approfondie via des structures non linéaires ou des interactions temporelles. Malgré ces limites, ce travail contribue à enrichir la compréhension économique des cyber-risques et met en avant l'importance stratégique de la gouvernance, de la numérisation maîtrisé et de l'investissement technologique. Les résultats présents des implications concrètes pour les décideurs publics : nécessité de renforcer les capacités de détection, d'accompagner l'innovation par des normes de cybersécurité, et de développer des stratégies nationales intégrées de gouvernance numérique. Pour les recherches futures, plusieurs pistes se dégagent : intégrer des

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

données microéconomiques ou transactionnelle, mobiliser des techniques d'IA pour la détection automatique des anomalies, construire des indicateurs composites via l'ACP, ou encore appliquer des modèles dynamiques GMM afin de mieux saisir les effets retardés des investissements en cybersécurité. En définitive, cette étude souligne l'urgence d'une approche économique structurée, combinant méthodes économétriques rigoureuses et innovations technologiques, pour anticiper et atténuer les coûts croissants des cybermenaces dans un monde de plus en plus interconnecté.

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

BIBLIOGRAPHIE

- **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. In R. Böhme & T. Moore (Eds), The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-030-14506-9_9
- **A**nderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12
- **B**iener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158. https://doi.org/10.1057//gpp.2014.19
- **B**ratik, A. W., Bertrand, M., Cullen, Z. B., Glaeser, E. L., Luca, M., & Stanton, C. T. (2020). The impact of COVID-19 on small business outcomes and expectations. Proceedings of the National Academy of sciences, 117(30), 17656-17666. https://doi.org/10.1073/pnas.2006991117
- **B**reiman, L. (2021). Random forests. Machine Learning, 45(1), 5-32. https://doi.org/10.1023/A:1010933404324
- **B**aryshnikov, Y. (2018). Cyber risk insurance: A market solution to a market problem. Journal of Risk and Insurance, 85(4), 967-988. https://doi.org/10.1111/jori.12227
- **C**hernykh, L., Howell, S. T., & Mandenko, K. (2021). Pandemic-induced digitalization and cyber risks in health and education sectors. Journal of Economic Behavior & Organization, 191, 850-867. https://doi.org/10.1016/j.jebo.2021.09.022
- **C**ameron, A. C., & Trivedi, P. K. (1990). The information matrix test and its applied alternative hypotheses. Journal of Econometrics, 47(1), 115-148. https://doi.org/10.1016/0304-4076(90)90085-R
- **E**NISA. (2021). ENISA Thread Landscape 2021: The year in review. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
- **I**MF. (2020).The macroeconomics of cyber risk: shocks and resilience. International Monetary Fund. https://www.imf.org
- **I**BM Security. (2023, 2024, 2025). Cost of Data Breach Report 2023, 2024, 2024. IBM Security. https://www.ibm.com/security/data-breach
- **I**nterpol. (2020). Interpol report on cybercrime in the COVID-19 era. Interpol. https://www.interpol.int & ENISA. (2021). ENISA Thread Landscape 2021: The year in review. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

- IBM Security. (2021), Cost of a Data Breach Report 2021. IBM Security. https://www.ibm.com/security/data-breach
- International Organization for Standardization. (2012). ISO/IEC 27032:2012-Information technology-Security techniques-Guidelines for cybersecurity. ISO. https://www.iso.org/standar/44375.html
- IBM Security. (2023). Cost of Data Breach Report 2023. IBM Security. https://www.ibm.com/security/data-breach & World Bank. (2024). Cybersecurity economics for emerging markets. World Bank Group. https://www.worldbank.org & ENISA. (2023). ENISA Thread Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
- IMF.(2020). The macroeconomics of cyber risk: shocks and resilience. International Monetary Fund. https://www.imf.org & Biener, C., Eling, M., & Wirfs, J.H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40(1), 131-158. https://doi.org/10.1057/gpp.2014.19
- McAfee,(2021). The hidden costs of cybercrime. McAfee Enterprise &Centre for Strategic and International Studies (CSIS). https://www.mcafe.com
- Mirsky, Y., & Shabtai, A. (2021). Deep learning for cyber security: Challenges and opportunities. IEEE Transactions on Dependable and Secure Computing, 18(2), 982-995. https://doi.org/10.1109/TDSC.2020.2973659
- Nguyen, T., & Kim, H. (2020). Predicting the economic impact of DDoS attacks with neural networks. Journal of Information Security and Applications, 54, 102556. https://doi.org/10.1016/j.jisa.2020.102556
- OECD. (2021). The COVID-19 crisis and cyber security policy responses. OCDE Publishing. https://www.oecd.org
- Organisation de coopération et de développement économiques. (2015). OECD regulatory policy outlook 2015. OCDE Publishing. https://doi.org/10.1787/9789264238770-en
- Organisation de coopération et de développement économiques. (2019). OCDE principales on Artificial intelligence. OCDE. https://www.oecd.org/going-digital/ai/principales
- Organisation de coopération et de développement économiques. (2021). Economic aspects of cybersecurity: The costs of (in) security. OCDE Publishing. https://doi.org/10.1787/5K420q9vwr8g-en
- Kopp, E., Leigh, A., & Wilson, C.(2017). Cyber risk, market failures, and financial stability (IMF Working Paper No. 17/185). International Monetary Fund. https://www.imf.org/en/Publications/WP/Issues/2017/07Cyber-Risk-Market-Failures-and-Financial-Stability-45103

African Scientific Journal
ISSN : 2658-9311
Vol : 03, Num 33 Décembre 2025

- **K**opp, E., Leigh, D., Luca, A., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund (IMF) Staff Discussion Note, SDN/17/05. https://doi.org/10.5089/9781484315224.006
- **K**opp, E., Kaffenberger, L., & Wilson, C. (2017).Cyber risk, market failures, and financial stability. Journal of Financial Stability, 34, 52-60. https://doi.org/10.1016/j.jfs.2017.03.001
- **K**shetri, N. (2016). Cybersecurity and international relations. Third World Quarterly, 37(5), 832-853. https://doi.org/10.1080/01436597.2015.1116363
- **S**haukat, K., Luo, S., Varadharaajan, V., Hameed, I.A., & Xu, M. (2020). Cyber threat detection using machine learning: Comparative analysis. Computers & Security, 99, 102104. https://doi.org/10.116:j.cose.2020.102104 & **R**omanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121-135. https://doi.org/10.1093/cybsec/tyw001
- **S**haukat, K., Luo, S., Varadharaajan, V., Hameed, I.A., & Xu, M. (2020). Cyber threat detection using machine learning: Comparative analysis. Computers & Security, 99, 102104. https://doi.org/10.116:j.cose.2020.102104
- **W**ooldridge, J.M. (2019). Introductory econometrics: A modern approach (7th ed.). Cengage learning. & United Nations Statistics Division. (2020). Handbook on statistical organization: Third edition—The operation and organization of a statistical agency. United Nations. https://unstats.un.org/unsd/publication/seriesf_88e.pdf
- **W**orld Bank. (2022). World Development report 2022: Finance for an equitable recovery. World Bank. https://doi.org/10.1596/978-1-4648-1730-4
- **W**orld Economics Forum. (2020). Global risks report 2020. WEF. https://www.weforum.org/reports/the-global-risks-report-2020