CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes de synthèse

Vol. 4, Num. 9
2024

Mesurer la cybercriminalité: perspectives internationales

Maya Dubord, candidate à la maîtrise en criminologie

Introduction

Toutes les organisations ne partagent pas une même vision de la cybercriminalité. Selon la littérature scientifique, **cette disparité crée des écarts dans la définition et donc la comptabilisation des cybercrimes** [1, 2]. La complexité des cyberattaques et l'évolution rapide du cyber écosystème criminel rendent difficile la production d'études représentatives [1, 2]. Cette note de synthèse présente **les résultats des principales études produites par des organisations internationales et quelques entreprises sur la cybercriminalité dans le but de quantifier celle-ci**. De plus, une attention particulière est portée à la méthodologie employée par chacun de ces rapports afin de mieux apprécier la robustesse des résultats qu'ils présentent. Leurs points forts et limites sont également détaillés.

Organisations internationales

Cette section présente les principaux rapports portant sur la cybercriminalité produits par des organisations internationales.

Internet Organized Crime Threat Assessment 2023 [3]

L'*Internet Organized Crime Threat Assessment 2023* est un rapport annuel produit par Europol. Dans cette neuvième édition, le rapport présente **les dernières tendances en matière de cybermenaces et les impacts de la cybercriminalité dans l'Union européenne (UE).** Les données collectées proviennent des membres de l'UE et de ses partenaires. **Ce rapport s'appuie sur l'expertise de professionnels de la cybersécurité et de données collectées en sources ouvertes**. Les analyses du rapport sont basées sur des indicateurs développés par Europol. Bien qu'il y ait peu d'informations sur le contenu des questionnaires et sur leur analyse, le rapport se concentre sur l'évolution des acteurs, des réseaux et des stratégies criminelles, ainsi que les infrastructures impliquées dans des cyberattaques.

Dans ce rapport de 2023, les principaux résultats démontrent que **les données volées par des cybercriminels peuvent servir de monnaie d'échange sur les marchés illicites**. Les stratégies employées pour la fraude et le vol de données sont partagées sur des forums de discussion sur le darkweb. **Les informations de carte de crédit ne sont plus les seules ciblées dans les cyberattaques**, car les informations personnelles dynamiques, telles que les données de géolocalisation, les activités en ligne récentes et les données de santé en temps réel, représentent maintenant une grande source d'intérêt pour les acteurs illicites. De plus, un individu peut être victime d'un cybercrime plusieurs fois et ses informations peuvent être

volées par plusieurs personnes. L'argent récolté par la fraude est blanchi grâce à des mules, des cryptomélangeurs* et des réseaux de blanchisseurs professionnels. En outre, les rançongiciels demandant des paiements par cryptomonnaies rendent difficile le traçage des cybercriminels par les organisations policières.

Ce rapport informe bien sur l'évolution des cybermenaces et permet d'orienter les décisions stratégiques, les politiques et les choix tactiques de lutte contre le cybercrime. Il permet d'avoir une vue d'ensemble des tendances européennes sur la cybercriminalité. Toutefois, le rapport fait peu mention de la méthodologie employée pour analyser les sources de données, des caractéristiques de l'échantillon et de la participation des pays. Bien que de nombreuses informations et tendances soient présentées dans le rapport, **peu de statistiques originales provenant des bases de données des organisations membres d'Europol viennent appuyer les constatations**. Il est donc difficile d'évaluer le degré de représentativité du rapport.

2022 Interpol Global Crime Trend Summary Report [6] et le Annual Report 2022 [7]

Le *2022 Interpol Global Crime Trend Summary Report* identifie **les tendances internationales et les préoccupations des États en matière de cybercriminalité**. Les données employées proviennent des 195 états membres d'Interpol et de certaines organisations appartenant au secteur privé. Le rapport démontre que **la fraude financière représente un haut ou très haut niveau d'inquiétude pour la communauté internationale**. Après la pandémie de COVID-19, la dépendance grandissante aux technologies numériques a mené à une hausse importante de l'utilisation de l'ingénierie sociale dans les fraudes en ligne. Les rançongiciels, l'hameçonnage, la fraude en ligne et l'accès non autorisé à des ordinateurs font partie des plus grandes préoccupations des États. **En Amérique du Nord, le blanchiment d'argent est perçu comme étant le plus gros risque pour la sécu-rité alors que ce risque apparaît en deuxième position en Europe après les risques liés au crime organisé.**

De manière générale, **ce rapport permet une comparaison entre plusieurs régions du monde et démontre clairement que la fraude est un des problèmes les plus importants rencontrés par les États**. Bien qu'il ne représente pas une étude exhaustive, ce rapport permet de comprendre certaines tendances de la cybercriminalité. Aucune statistique officielle n'est présentée, mais le rapport contient des graphiques identifiant les préoccupations principales des États de manière hiérarchisée. Le rapport permet donc d'avoir une vue d'ensemble des préoccupations principales des pays membres plutôt que de présenter un portrait global de la cybercriminalité.

Le *Annual Report 2022* publié en 2023 par Interpol partage les mêmes objectifs et sources de données que le rapport précédent. **Ce document présente, en revanche, des statistiques sur les opérations de recouvrement des fonds qui ont été effectués**. Pour l'année 2022, **200 millions de dollars provenant de cyberfraude ont été interceptés par différents partenaires**. Les mêmes limites méthodologiques présentes dans le rapport précédent sont aussi présentes dans celui-ci. En revanche, ce rapport propose une plus grande quantité de statistiques.

*Les crypto mélangeurs permettent une plus grande anonymisation de la cryptomonnaie. Ils permettent de prendre le contenu de plusieurs portefeuilles, de les mélanger et de les redistribuer à chacun de leurs utilisateurs en fonction des montants prélevés. Ainsi, il n'est plus possible de retracer les portefeuilles originaux des utilisateurs. Sans analyses plus avancées, seul l'identifiant du crypto mélangeur devient retraçable [4, 5].

Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique : Perspectives du bureau pour les opérations de lutte contre la cybercriminalité en Afrique [8]

Le *Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique* analyse **les cybermenaces les plus présentes sur le territoire africain et brosse un portrait des initiatives nationales de prévention des risques de cyberattaques**. Plusieurs recommandations de mesures de cyberrésilience à mettre en place sont aussi présentées. Dans le cadre de la collecte de données, **46 pays africains membres d'Interpol ont été sondés**. Il s'agit d'un excellent taux de réponse, soit **plus de 80 % des États africains**. Le questionnaire employé comporte 40 questions qualitatives et quantitatives dans lequel **différents thèmes y sont abordés tels que la prévention, la détection, les processus d'enquêtes et les mesures de répression employées**. Dans le but de soutenir les données rapportées par les questionnaires, d'autres partenaires du secteur privé et public ont participé à la collecte tels que des agences gouvernementales allemandes et britanniques ou bien encore Shadowserver, Trend Micro, Kaspersky, Paloalto et Group-IB. En revanche, aucune information n'est disponible sur la forme de leur participation.

Les principaux résultats du rapport démontrent que **les infractions liées au numérique sont perçues comme étant un risque moyen à élevé dans les 2/3 des autorités sondées**. Le nombre moyen d'incidents hebdomadaires par organisation ayant eu lieu sur le territoire africain en 2023 serait le plus élevé au monde. Entre 2022 et 2023, il y aurait eu une augmentation de 23 % de ce type d'événements. **Les attaques par logiciels malveillants, incluant les rançongiciels, restent la principale forme de cybercrime sur le territoire** et les menaces qu'elles présentent contre les infrastructures critiques restent une source importante de préoccupations.

Ce rapport offre plusieurs avantages, notamment puisqu'il présente les caractéristiques des attaques par logiciels malveillants qui sont les plus fréquemment recensés par les États africains. Les recommandations de mesures ayant pour but de favoriser la cyberrésilience offrent des stratégies concrètes et applicables à différentes tailles d'organisations. En revanche, **peu de statistiques sont offertes sur la prévalence des cyberattaques sur le territoire**. Il reste donc difficile de cibler l'ampleur du problème. Le processus de traitement des données et le contenu des questionnaires ne sont que vaguement expliqués. Il est donc difficile de comparer ce rapport à d'autres études.

ENISA Threat Landscape

L'*ENISA Threat Landscape 2023* a été publié par l'Agence européenne pour la cybersécurité en 2023. Créée en 2004, l'ENISA assure le renforcement de la cybersécurité de l'Europe, notamment par le développement de certifications, de produits et services numériques et le partage des connaissances sur les meilleures pratiques en matière de résilience des infrastructures numériques [10]. Le but du rapport est d'analyser **les tendances internationales de la cybercriminalité et des cybermenaces auxquelles sont confrontés les États**. Pour y arriver, **des données provenant de sources ouvertes et de documents classifiés sur les cybermenaces sont mobilisées**. La méthode d'analyse de chacune des sections du rapport est présentée avant celles-ci. **Près de 25 000 incidents ont été répertoriés dans une base de données maison**. Des sources universitaires et médiatiques sont aussi employées pour corroborer certaines informations dont la fiabilité ne pouvait pas être confirmée.

Pour tous les secteurs économiques confondus, **les menaces principales identifiées lors des analyses des incidents sont les rançongiciels (32,32 %), les menaces contre les données (20,09 %), les attaques par déni de service (21,4 %) et l'ingénierie sociale (7,88 %)**. Une augmentation de l'utilisation d'outils technolo-

-giques légitimes dans les cybercrimes y est également notée. On assisterait aussi à **la professionnalisation des acteurs malveillants**. L'hameçonnage a été identifié comme étant la porte d'entrée la plus fréquente pour commettre des cybercrimes et le courriel reste la plateforme la plus fréquemment exploitée par les acteurs malveillants. **L'intelligence artificielle serait de plus en plus employée pour préparer des attaques**. Les attaques via la chaîne d'approvisionnement numérique (*supply chain*) sont de plus en plus fréquentes et ciblent principalement les développeurs et administrateurs de plateformes. **Le secteur financier est visé dans 6 % des cyberattaques où les attaques par déni de service y sont les plus fréquentes, suivies de celles par rançongiciels**. Le rapport inclut aussi une présentation des groupes cybercriminels les plus actifs et des techniques d'attaques émergentes.

La méthodologie du rapport s'appuie sur **un processus de validation des résultats par d'autres organisations qui augmente la fiabilité des données et de leurs interprétations**. Les analyses présentées incluent des statistiques portant sur l'Union européenne et un volet international. Les données se basent sur des incidents de cybersécurité de petite et grande envergure. Aussi, il se concentre sur plusieurs secteurs économiques d'intérêts. Bien que les données couvrent une impressionnante partie de l'écosystème criminel, il arrive tout de même à garder un haut niveau de précision statistique. Le rapport est facile à lire et est accessible pour des individus sans connaissance sur la cybercriminalité ou en informatique. Il est, en revanche, très long et n'est pas nécessairement destiné au grand public.

Global Risk Report

Le *Global Risk Report* a été publié en 2024 par le World Economic Forum (WEF), dont l'objectif est de présenter **les prédictions envisagées par des experts académiques, professionnels ou gouvernementaux sur les cybermenaces potentielles autour du monde**. Le WEF est un groupe de réflexion communément appelé *think tank*, qui vise une meilleure collaboration entre les secteurs privé et public autour du monde [12]. **Un sondage a été effectué auprès de 1490 individus actifs au sein de la communauté de la cybersécurité**. Des données du *Executive Opinion Survey* regroupant 11 000 entreprises de 113 économies différentes ont aussi été utilisées. Finalement, **55 experts du WEF et 160 experts de la communauté de la cybersécurité** ont partagé leurs impressions par le biais de rencontres et ateliers thématiques.

Les principales constatations du rapport présentent des **projections négatives pour les deux prochaines années**. Se divisant en quatre axes principaux (changements climatiques, bifurcation démographique, accélération technologique et changements géostratégiques), les experts concluent que d'importantes périodes d'instabilité sont à venir. **Les cyberattaques sont vues comme étant la cinquième menace la plus importante pour 2024**. **Les enjeux liés au numérique font partie du top 10 des menaces perçues comme étant les plus importantes pour les 10 prochaines années**. **Les risques liés à l'utilisation de l'intelligence artificielle pour lancer des cyberattaques sont projetés comme étant susceptibles d'augmenter au cours des dix prochaines années**. L'utilisation d'un seul fournisseur d'intelligence artificielle dans le secteur de la finance pourrait augmenter les risques de paralysie des infrastructures critiques et créer d'importantes vulnérabilités aux cyberattaques. **Une attention particulière doit être portée à l'évolution des ordinateurs quantiques dans les prochaines années qui pourraient être employés à des fins criminelles**.

Ce rapport permet de mettre en lumière les principales préoccupations et projections des décideurs publics et privés en matière de cybersécurité sur un, deux et dix ans. Des représentations graphiques permettent de visualiser les principaux enjeux auxquels sont confrontés les différents pays. Bien qu'il s'agisse d'experts en cybersécurité, **ces résultats dépen-**

-dent de perceptions individuelles et restent spéculatifs jusqu'à un certain point. Ils permettent donc d'avoir une vue d'ensemble de phénomènes à surveiller, mais pas de faire un état de la situation actuelle.

Indice mondial de cybersécurité 2020 [13]

L'*Indice mondial de cybersécurité 2020* **mesure l'engagement des pays en matière de cybersécurité, leurs vulnérabilités et le développement de bonnes pratiques de prévention**. Il a été développé par l'Union internationale des télécommunications des Nations Unies. La plus récente édition du rapport a été publiée en 2021. Des données ont été collectées par questionnaires auprès de 194 États. **Le sondage comporte 82 questions, divisées en 20 indicateurs reposant sur 5 piliers principaux : les mesures juridiques, techniques, organisationnelles, le renforcement des capacités et la coopération**. Une note maximale de 20 points peut être accordée à chacun des piliers pour un total de 100 points. Pour les pays n'ayant pas participé au sondage, une analyse documentaire a été effectuée dans le but de compléter les données, ce qui implique que, pour certains États, les informations présentées pourraient donc manquer de précision.

Les principaux résultats démontrent que **97 des 194 États sondés possèdent un cadre législatif portant sur la protection des données personnelles**. 116 auraient mis en place un programme de sensibilisation en matière de cybersécurité pour les petites et moyennes entreprises. **Le Canada s'est vu attribuer une note globale de 97,67/100 points**. Ces domaines de force identifiés sont les **mesures juridiques, organisationnelles et la coopération**. En revanche, **des améliorations pourraient avoir lieu au niveau des mesures techniques**.

La méthodologie employée pour construire l'indice mondial de cybersécurité est clairement expliquée et le taux de réponse des États est excellent. **Le rapport permet de mettre en lu-mière les initiatives mises en place à l'international en matière de cybersécurité, notamment en matière de formation et d'audit**s. En revanche, des changements méthodologiques ont été apportés entre la présente édition du sondage et la précédente. Ainsi, **les comparaisons d'année en année deviennent difficiles**. Il est aussi possible que des États aient tenté de surévaluer les initiatives qu'ils ont mises en place créant certains biais d'analyse.

Organisations privées

La prochaine section présente les rapports ayant été produits par des organisations privées sur les tendances en matière de cybercriminalité.

2024 Data Breach Investigations Report [14]

Le *2024 Data Breach Investigations Report* publié par Verizon Business en 2024 établit un **portrait des acteurs, tactiques, et cibles principales des cybercriminels pour 2023**. Pour y arriver, **une base de données de près de 10 000 incidents de cybersécurité ayant eu lieu entre novembre 2022 et 2023 a été analysée**. Ce rapport est produit annuellement depuis 2008 [15] et **porte uniquement sur les attaques contre les entreprises et les organismes publics**. Les attaques contre les individus n'y sont pas abordées.

Les principaux résultats d'analyse démontrent que **près du tiers des brèches de données ayant eu lieu en 2023 impliquaient l'utilisation d'un rançongiciel**. Ces derniers seraient perçus comme une menace pour 92 % des entreprises. **68 % des incidents de cybersécurité impliquaient un élément humain** et près du tiers des brèches de données ont été causées par une erreur humaine. De plus en plus d'individus travaillant au sein des entreprises sont responsables d'incidents de cybersécurité. En 2023, 35 % des incidents ont été causés par des membres internes aux organisations. Le gain financier reste le principal motif des cybercriminels pour perpétrer des attaques.

L'intelligence artificielle est perçue comme pouvant devenir un outil facilitateur des cyberattaques, mais il n'est pas anticipé qu'elle puisse remplacer complètement les compétences nécessaires à la création de rançongiciels ou de logiciels malveillants. De manière générale, le rapport présente une méthodologie assez claire. Sa force principale est de démontrer les types d'incidents les plus fréquemment répertoriés par Verizon. En revanche, **peu d'informations sont disponibles sur les pays dans lesquels ont eu lieu les incidents**. La division des analyses en sections portant sur les acteurs, les biens, les actions et les attributs est intéressante. Un volet analytique plus approfondi plutôt qu'une présentation étendue des données aurait permis de mieux contextualiser les résultats et de dégager des recommandations applicables en matière de prévention.

X-Force Threat Intelligence Index 2024 [16]

Le *X-Force Threat Intelligence Index 2024* brosse un portrait de la cybercriminalité dans le monde et a été publié par IBM en 2024. Pour y arriver, **des données ont été collectées au courant de l'année par un logiciel maison de détection des virus**. Il s'agit d'un rapport extrêmement complet sur les tactiques employées par les acteurs malveillants dans leurs cyberattaques. Un volet est dédié aux impacts des cyberattaques sur les entreprises. Des données divisées par secteurs d'activités et par région du monde s'y retrouvent aussi.

Les principaux résultats du rapport démontrent que **les attaques employant des accréditations valides sont en augmentation de 71 %, mais que l'utilisation de rançongiciel est en baisse de 11,5 %**. Près du tiers des incidents impliquaient un vol ou une fuite de renseignements. **L'utilisation de « voleurs d'informations » (*infostealers*),** un type de logiciel malveillant, **a vu une augmentation fulgurante de 266 % dans la dernière année**. Le tiers des vulnérabilités qui ont été exploitées au sein des entreprises a été identifié comme ayant été causé par de mauvaises configurations des infrastructures numériques. **Dans 84 % des cas, les attaques contre ces infrastructures ayant employé un accès initial par vecteur (hameçonnage, comptes valides, etc.) auraient pu être prévenues. Les attaques par hameçonnage seraient en baisse de 44 % depuis l'année précédente.** Cette baisse pourrait être causée par les efforts de plus en plus importants pour produire des courriels d'hameçonnage, le rapport estimant qu'il faut en moyenne 16 heures de travail humain pour arriver à produire un courriel malveillant efficient.

Les **principaux impacts** des cyberattaques sur les entreprises identifiées dans le rapport sont **le vol et les fuites de données (32 %), l'extorsion (24 %), une baisse de la réputation de l'organisation (9 %) et la destruction de données (9 %)**. Le secteur de la finance et des assurances a été ciblé par des cyberattaques dans 18,2 % des cas, soit une faible augmentation de 1,2 % par rapport à 2019. 38 % des incidents dans cette industrie impliquaient un logiciel malveillant et 25 % des rançongiciels. **L'hameçonnage était la porte d'entrée la plus fréquemment employée par les acteurs illicites**. Plusieurs méthodes de prévention des cyberattaques sont présentées dans le rapport incluant la connaissance des vulnérabilités internes, notamment face aux attaques par accréditation valide, le développement de protocoles d'intervention en matière de cybersécurité et le test des vulnérabilités des infrastructures pour tenter de les consolider.

De manière générale, ce rapport est très complet, offrant **une foule d'informations, tant sur les actions posées par les acteurs malveillants que sur les conséquences de celles-ci**. Le document est clair et divisé d'une manière logique et pertinent pour sa compréhension. En revanche, **il est nécessaire d'avoir certaines bases de connaissances en informatique ou sur la cybercriminalité pour comprendre certains termes techniques**. Il est donc plutôt destiné à des professionnels qu'au public général.

The 2024 Crypto Crime Report [17]

Le *2024 Crypto Crime Report* a été publié par l'entreprise Chainalysis en 2024. Ce document brosse un portrait de la criminalité internationale liée à la cryptomonnaie. Plusieurs thématiques sont abordées telles que le blanchiment d'argent, la manipulation des marchés, les marchés illicites sur le *darkweb*, le financement des organisations terroristes, les rançongiciels et le contenu numérique lié à l'exploitation sexuelle d'enfants.

Selon ce rapport, **24,2 milliards de dollars auraient transité par des portefeuilles illicites en 2023**. Bien que **de plus en plus de cybercrimes impliquent des *Stablecoins***, la vente sur les marchés illicites et les rançongiciels ont lieu plus fréquemment en Bitcoins**. **Le blanchiment d'argent serait en baisse, mais les revenus des marchés illicites seraient quant à eux en hausse.** Le vol de fonds resterait aussi une menace importante et les attaques par rançongiciels sur les infrastructures critiques seraient en hausse.

Ce rapport présente une quantité impressionnante de statistiques, d'analyses et d'études de cas. **Il permet de donner une idée assez précise des tendances de l'écosystème cybercriminel et de la prévalence des cybercrimes**. Bien que la nature anonyme des cryptomonnaies rende difficile la validation totale de la fiabilité des données, la méthodologie employée permet une certaine forme de triangulation. Le rapport, publié annuellement, s'est raffiné, devenant de plus en plus complet et approchable. Une plus grande partie du document est maintenant octroyé à la mise en contexte des analyses et statistiques. **Des connaissances de base sur les cryptomonnaies peuvent être nécessaires à la compréhension de certaines sections**.

Conclusion

Cette note de synthèse présente les principaux rapports sur la cybercriminalité et produits par les organisations internationales et privées. Bien que **les sources de données soient nombreuses, il reste difficile d'obtenir des statistiques fiables sur la prévalence des cyberattaques dans le monde**. De plus, **peu des études présentées dans cette note s'intéressent aux cybercrimes contre les individus en s'appuyant sur des statistiques de première main**, **même lorsqu'ils sont produits par des organisations policières internationales**. Ces institutions devraient, en théorie, avoir accès à de telles données. Certaines études se concentrent sur les attaques ayant eu lieu dans les dernières années, tandis que d'autres se penchent plutôt sur les préoccupations des États face à des cybermenaces. Toutes les études recensées ont de nombreux avantages, mais possèdent aussi d'importantes limites méthodologiques, notamment l'opacité des démarches d'analyses ou de construction des outils de collecte de données. Ainsi, **il est nécessaire de continuer à produire des rapports les plus complets et d'analyser critiquement ceux disponibles**. Les difficultés liées à la définition et la catégorisation des cybercrimes rendent d'autant plus difficile l'homogénéisation de l'interprétation des résultats [1, 2].

****** Les Stablecoins sont des cryptomonnaies qui visent à offrir une alternative plus stable aux Bitcoins en associant leur valeur monétaire à celle d'une autre monnaie ou commodité financière [18].

Références

[1] Brinton, J., Langton, L., Krebs, C. et Casper, M. (2023). An Environmental Scan of Cybercrime Measurement: Recommendations for the National Crime Victimization Survey | Bureau of Justice Statistics (306766). *Bureau of Justice Statistics*.

[2] Junger, M. et Hartel, P. (2022). Crime Victimisation Surveys Measuring Cybercrime. Dans M. Aebi F., S. Caneppele et L. Molnar (dir.), *Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys: Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020* (p. 75–97). eleven.

[3] Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA) (978-92-95220-83–6)*. Publications Office of the European Union.

[4] Chainalysis. (2023, January 26). Four Exchange Deposits Received +$1B in Illicit Funds in 2022. *Chainalysis*.

[5] Hamilton, R. et Leuprecht, C. (2024). The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions. Dans D. Goldbarsht et L. de Koker (dir.), Financial Crime and the Law: Identifying and Mitigating Risks (p. 15–42). Springer Nature Switzerland.

[6] Interpol. (2022). *2022 Interpol Global Crime Trend Summary Report*. Interpol.

[7] Interpol. (2023). *Annual Report 2022*. Interpol.

[8] Bureau pour les opérations de lutte contre la cybercriminalité en Afrique. (2024). *Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique : Perspectives du Bureau pour les opérations de luttre contre la cybercriminalité 3ième édition*. Interpol.

[9] European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023 (Report/Study 978-92-9204-645–3)*. European Union.

[10] Union européenne. (n.d.). *Agence de l'Union européenne pour la cybersécurité*. Union européenne.

[11] World Economic Forum. (2024). *Global Risks Report 2024 (978-2-940631-64–3)*. World Economic Forum.

[12] World Economic Forum. (2024). *Our Mission*. World Economic Forum.

[13] Union internationale des télécommunications. (2021). *Indice mondial de cybersécurité 2020 (978-92-61-33922–7)*. Nations Unies.

[14] Verizon Business. (2024). *2024 Data Breach Investigations Report*. Verizon Business.

[15] Verizon Business. (2022). *2022 Data Breach Investigations Report Public Sector Snapshot*. Verizon Business.

[16] IBM. (2024). *IBM X-Force Threat Intelligence Index 2024*. IBM.

[17] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. Chainalysis.

18. Hayes, A. (2024). Stablecoins: Definition, How They Work, and Types. *Investopedia*.