INTERPOL

RAPPORT INTERPOL SUR L'ÉVALUATION DES CYBERMENACES EN AFRIQUE 2025

4ÈME ÉDITION

MAI 2025

AVERTISSEMENT

TABLE DES MATIÈRES

Neal Jetton
Directeur de la
Cybercriminalité
INTERPOL

AVANT-PROPOS D'INTERPOL

Le continent africain se trouve à un moment charnière de son évolution sur le plan numérique. À mesure que la connectivité s'améliore et que l'innovation numérique s'accélère dans la région, celle-ci est confrontée à des cybermenaces de plus en plus complexes. Ces menaces ne connaissent pas de frontières. Passant d'un pays à l'autre, elles évoluent rapidement et sont de plus en plus perfectionnées. Elles prennent pour cible le socle même du progrès : les systèmes financiers, les services publics, les infrastructures critiques et, surtout, la confiance des citoyens dans l'avenir numérique.

Cette quatrième édition de l'évaluation d'INTERPOL sur les cybermenaces en Afrique donne un aperçu indipsensable de la situation actuelle. S'appuyant sur des renseignements opérationnels, de nombreuses informations fournies par les services chargés de l'application de la loi et une collaboration stratégique avec le secteur privé, ce rapport brosse un tableau précis des menaces actuelles. Dans ce panorama en constante évolution, les logiciels malveillants, en particulier les rançongiciels, les escroqueries en ligne, notamment par hameçonnage, ainsi que les escroqueries aux faux ordres de virement continuent d'être sur le devant de la scène. Cependant, il faut également s'attaquer sans tarder aux nouveaux dangers qui se profilent, tels que la fraude portée par l'IA, les abus sexuels en ligne à partir d'images et les infractions numériques à caractère sexuel, sans oublier la cybercriminalité en tant que service.

Chez INTERPOL, nous sommes conscients qu'aucune institution ni aucun pays n'est en mesure de relever seul ces défis. L'ampleur et la rapidité avec laquelle la cybercriminalité évoluent exigent une réponse unifiée, coordonnée et fondée sur le renseignement. Dans le cadre de l'opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC) et en lien étroit avec AFRIPOL, nous renforçons nos capacités opérationnelles, entretenons la confiance entre les services de lutte contre la cybercriminalité des différents pays et favorisons des initiatives transfrontalières de coopération capables de déjouer efficacement les réseaux cybercriminels.

Par ailleurs, ce rapport met en évidence la résilience de plus en plus forte et les capacités croissantes des services chargés de l'application de la loi en Afrique. Des progrès sont en effet constatés à plusieurs niveaux, avec des opérations régionales couronnées de succès, de nouvelles réformes législatives et un renforcement des capacités. Mais il reste encore un long chemin à parcourir. Le manque de maîtrise numérique, d'harmonisation législative, de moyens d'enquête et d'accès aux éléments de preuve numériques continue de compromettre l'efficacité de ces services.

Le présent rapport se veut à la fois un appel à l'action lancé à tous nos partenaires, qu'ils relèvent des forces de l'ordre, de l'administration, du secteur privé ou de la société civile, et une base pour la collaboration. Ce n'est qu'en travaillant coude à coude, en partageant nos connaissances et en instaurant une confiance mutuelle entre les pays et les différents secteurs concernés que nous pourrons garantir l'avenir numérique de l'Afrique.

Je souhaite exprimer ma sincère reconnaissance au Desk Africain pour les Opérations de Lutte contre la Cybercriminalité pour les opérations de lutte contre la cybercriminalité en Afrique et à toutes les personnes qui ont contribué à ce rapport. Vos efforts renforcent notre détermination collective à bâtir un environnement numérique plus sûr et plus résilient pour tous. Pour conclure, je tiens à remercier la communauté policière de nos pays membres africains pour son dévouement à la lutte contre la cybercriminalité et les efforts qu'elle déploie pour rendre le monde plus sûr.

M. Jalel Chelba, ambassadeur
Directeur exécutif
par intérim d'AFRIPOL

AVANT-PROPOS D'AFRIPOL

L'Afrique entre aujourd'hui dans une ère de transformation numérique rapide, offrant des opportunités sans précédent pour le développement économique, social et institutionnel des pays du continent. Cette dynamique est le reflet d'une volonté collective d'accélérer l'inclusion numérique, d'améliorer les services publics et d'encourager l'innovation dans ces pays. Toutefois, ces avancées majeures vont de pair avec des menaces de plus en plus complexes qui se répandent dans le cyberespace, mettant en danger la sécurité des États, des infrastructures critiques, des entreprises et des citoyens africains.

Face à ces difficultés, AFRIPOL s'impose comme une organisation de premier plan sur le continent, en mesure d'apporter une réponse coordonnée, ambitieuse et adaptée au contexte africain. Notre engagement est clair : nous voulons promouvoir une souveraineté numérique forte, capable de protéger efficacement nos sociétés contre des cybermenaces de plus en plus élaborées, qui transcendent souvent les frontières et évoluent aussi rapidement que la technologie elles-même.

En 2024, AFRIPOL a multiplié ses activités en coopération étroite avec INTERPOL, les structures régionales spécialisées, les agences nationales chargées de la sécurité et des partenaires stratégiques du secteur privé. Des interventions conjointes de grande envergure, comme l'opération Serengeti, ont abouti au démantèlement de réseaux criminels très évolués, spécialisés dans les rançongiciels, les escroqueries financières, l'hameçonnage ciblé et les attaques contre les systèmes d'information de l'administration publique. Ces succès opérationnels soulignent toute l'importance de la coopération interservices, du partage d'informations, de la mise en commun des capacités et d'une action coordonnée à l'échelle du continent.

Dans le même temps, AFRIPOL a continué de renforcer les compétences du personnel des services chargés de l'application de la loi grâce à des programmes de formation spécialisés et ciblés, portant sur des domaines clés tels que l'analyse de renseignements criminels, le traçage des flux financiers illicites, les enquêtes numériques, la cybersurveillance et la protection des infrastructures critiques. Les accords stratégiques conclus avec Kaspersky et Group-IB en 2024 ont posé un nouveau jalon dans notre démarche visant à doter les États membres des moyens nécessaires pour prévenir les incidents majeurs et y répondre, en améliorant leur accès aux outils technologiques, aux renseignements sur les menaces et à l'expertise internationale.

À partir de 2025, AFRIPOL centrera ses efforts sur trois grandes priorités stratégiques : 1) renforcer la coopération internationale et interafricaine en vue de répondre de manière cohérente aux menaces transnationales ; 2) aider activement les États membres à renforcer leurs capacités opérationnelles, humaines et technologiques ; et 3) intégrer systématiquement les innovations, en particulier les technologies de l'intelligence artificielle et de la chaîne de blocs, afin d'anticiper les risques et d'adapter nos stratégies en temps réel.

La cybersécurité n'est pas qu'une simple question technique. Elle est devenue un pilier incontournable de la stabilité, de la paix et du développement durable en Afrique, comme le souligne l'Agenda 2063. Elle est directement liée à la souveraineté numérique des États, à la résilience de nos institutions, à la confiance des citoyens et au bon fonctionnement de nos économies. C'est dans cet esprit de responsabilité partagée, de solidarité entre les pays du continent et d'innovation continue qu'AFRIPOL renouvelle son engagement à construire un cyberespace africain sûr, inclusif, souverain et résilient au service de la paix, de la sécurité et du progrès collectif.

SIGLES ET ACRONYMES

AFJOC	Opération conjointe de lutte contre la cybercriminalité en Afrique
AFRIPOL	Mécanisme de coopération policière de l'Union africaine
IA	Intelligence artificielle
UA	Union africaine
FOVI	Escroquerie aux faux ordres de virement
CaaS	Cybercriminalité en tant que service
DDoS	Déni de service distribué
Go	Gigaoctet
TIC	Technologies de l'information et de la communication
ASEBI	Abus Sexuel En ligne Basé sur l'Image
SIM	Module d'identification de l'abonné
SMS	Service de messages courts
To	Téraoctet
UNESCO	Organisation des Nations Unies pour l'éducation, la science et la culture
USD	Dollar des États-Unis

REMERCIEMENTS

Le présent rapport a été préparé par le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique sous les auspices de l'opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC), et avec le financement du Bureau des Affaires étrangères, du Commonwealth et du Développement du Royaume-Uni (FCDO). Pour toute question concernant ce rapport, veuillez nous contacter à l'adresse suivante : AfricaDesk@interpol.int.

Ce rapport est le fruit d'une analyse exhaustive d'informations recueillies auprès d'un large éventail de sources, notamment des pays membres africains d'INTERPOL et de ses partenaires du secteur privé tels que Bi.Zone, Group-IB, Kaspersky et Trend Micro. En outre, les unités opérationnelles et de renseignement d'INTERPOL ont elles aussi été mises à contribution pour étayer le rapport, qui offre ainsi une vision complète et nuancée des problématiques soulevées.

Nous remercions chaleureusement les 43 des 54 pays membres africains qui ont répondu au questionnaire d'évaluation des cybermenaces et nous ont fourni des informations précieuses pour la rédaction du présent rapport.

RÉSUMÉ

La cybercriminalité prend actuellement de l'ampleur dans toute l'Afrique, menaçant la sécurité publique, les systèmes financiers et la confiance dans le numérique. Si de plus en plus de pays commencent à prendre des mesures face à ces cybermenaces, nombre d'entre eux connaissent encore de graves problèmes structurels qui entravent leur capacité à les déceler, à enquêter à leur sujet et à y mettre un terme.

Les capacités des services chargés de l'application de la loi varient d'un pays à l'autre. La majorité des pays font état d'un manque de formation aux techniques d'enquête sur la cybercriminalité, d'un accès limité aux outils de criminalistique numérique et d'une infrastructure insuffisante. Bien que plusieurs pays aient mis en place des unités spécialisées dans la cybercriminalité, celles-ci doivent souvent composer avec des moyens et des effectifs limités.

Les cadres juridiques s'améliorent, mais les progrès sont inégaux. Certains pays membres ont modernisé leur législation en matière de cybercriminalité. Toutefois, dans de nombreux cas, les pays ayant répondu au questionnaire signalent que leurs cadres juridiques et leurs capacités en matière de poursuites judiciaires laissent encore à désirer sur ce point. En outre, leur législation pourrait être davantage harmonisée avec les normes régionales et internationales. Ces lacunes continuent d'entraver les poursuites et la recevabilité des éléments de preuve numériques.

La coordination transfrontalière demeure un enjeu majeur. Alors que les opérations soutenues par INTERPOL ont donné de bons résultats, les pays signalent que le recours aux canaux de coopération officiels, notamment aux démarches d'entraide judiciaire, est encore minoritaire et laborieux. À cela viennent s'ajouter les problèmes juridictionnels, le manque de confiance et les difficultés d'accès aux plateformes numériques mondiales, qui sapent encore plus les efforts des services chargés de l'application de la loi dans la région.

Les nouvelles menaces évoluent rapidement. L'utilisation à des fins criminelles de l'intelligence artificielle et des contenus générés ou manipulés par celle-ci, ainsi que les escroqueries par téléphone portable, dépassent la capacité de réaction de nombreux services. Pour mettre leur dessein à exécution, les malfaiteurs tirent souvent parti de lacunes juridiques et opérationnelles. Afin de lutter contre ces menaces, il est donc nécessaire d'adopter de nouvelles formes de coopération interservices et de collaboration internationale.

Malgré tous ces défis, quelques signes encourageants ont été observés. Plusieurs pays membres ont renforcé les partenariats public-privé, mis à jour leur législation pour améliorer l'efficacité des poursuites face à la cybercriminalité et participé à des opérations régionales couronnées de succès. Il existe une prise de conscience croissante des risques liés à la cybercriminalité. En conséquence, les services de police nationaux sont de plus en plus nombreux à miser sur le renforcement de leurs capacités d'enquête dans le domaine numérique.

Ce rapport présente les principaux défis auxquels l'Afrique est confrontée en matière de cybercriminalité, les nouvelles tendances des menaces dans ce domaine et des exemples concrets d'obstacles systémiques et d'opérations réussies. Il conclut par une série de recommandations destinées à améliorer les capacités au niveau national, à renforcer les cadres juridiques et procéduraux et à approfondir la coopération internationale, trois facteurs déterminants qui sont le gage d'une résilience à long terme.

1. INTRODUCTION

Le coup d'accélérateur donné par l'Afrique sur la voie de la transformation numérique est en train de remodeler les économies, la gouvernance et la société. Alors que le continent commence à tirer parti des technologies et des innovations les plus récentes, son exposition à la cybercriminalité s'est aussi considérablement accrue. L'adoption du numérique va en effet de pair avec une multiplication des menaces pour les systèmes financiers, les services publics, les entreprises et les utilisateurs finaux.

C'est pour mieux cerner ces risques et leur évolution qu'INTERPOL a procédé à une évaluation des cybermenaces existantes à l'échelle du continent. Le présent rapport repose sur les données recueillies au moyen d'un **questionnaire détaillé envoyé aux services chargés de l'application de la loi des pays africains, ainsi que sur des renseignements opérationnels, des observations fournies par des partenaires d'INTERPOL issus du secteur privé et des informations provenant de sources publiques.** Cette approche fondée sur des sources variées permet d'obtenir une bonne vue d'ensemble des tendances régionales.

Le présent document fait suite au Rapport de 2024 sur l'évaluation des cybermenaces en Afrique et s'appuie sur les conclusions de ce dernier. Il entend montrer un instantané du panorama actuel de la cybersécurité et faire le point sur les progrès qui ont été accomplis pour relever les défis précédemment mis en évidence.

Ce rapport a pour vocation d'aider les services chargés de l'application de la loi, les responsables des politiques et les acteurs de la cybersécurité à détecter les nouvelles menaces, à combler les lacunes en matière de capacités et à renforcer la coopération aux niveaux national et régional. Les enquêtes sur la cybercriminalité, à quelque niveau que ce soit, ont une incidence directe sur les victimes effectives et potentielles partout dans le monde. Les efforts collectifs en faveur de la cybersécurité sont le gage d'un avenir numérique plus sûr en Afrique.

2. L'ÉVOLUTION DES CYBER-MENACES EN AFRIQUE

La transformation numérique rapide de l'Afrique a considérablement amélioré la connectivité du continent et favorisé l'adoption généralisée de technologies telles que les services bancaires mobiles, le commerce électronique et l'informatique en nuage, stimulant ainsi la croissance économique et l'innovation[1]. Cependant, cet essor va de pair avec certains défis pour la cybersécurité, étant donné que les infrastructures numériques deviennent des cibles de plus en plus attrayantes pour les individus mal intentionnés qui se livrent aux cyberattaques. Alors que la région compte désormais plus de 500 millions d'internautes, de nombreux pays n'ont toujours pas mis en place des mesures de cybersécurité adéquates, ce qui rend les entreprises et les particuliers vulnérables à ces attaques[2] Un peu partout sur le continent, des enjeux de taille aggravent ces risques : les cadres juridiques pour les contrer ne sont pas encore au point, les investissements en cybersécurité sont limités, et la maîtrise numérique est plutôt médiocre.

L'utilisation généralisée des smartphones a fait des plateformes mobiles une cible de choix pour les cyberescrocs, en particulier dans les régions où l'utilisation des services bancaires mobiles est très répandue. De plus, l'utilisation croissante des appareils connectés à l'Internet des objets dans des secteurs tels que l'agriculture, la santé et l'industrie manufacturière n'est pas sans risque pour la sécurité, car bon nombre de ces appareils ne sont pas suffisamment protégés[3]. Plusieurs États africains, dont l'Éthiopie, le Zimbabwe, l'Angola, l'Ouganda, le Nigéria, le Kenya, le Ghana et le Mozambique figurent parmi les pays les plus fréquemment ciblés au niveau mondial en 2024, selon les statistiques de détection des logiciels malveillants figurant dans l'Indice mondial de cybersécurité de l'Union internationale des télécommunications (UIT)[4]. Ce constat souligne à quel point il est aujourd'hui nécessaire de mettre en place des cadres plus solides pour garantir la cybersécurité, afin de préserver le développement numérique de la région et d'en assurer la résilience à long terme[5, 6].

Le Rapport INTERPOL de 2025 sur l'évaluation des cybermenaces en Afrique révèle que les actes de cybercriminalité sont en forte hausse sur l'ensemble du continent. Plus de deux tiers des pays africains membres d'INTERPOL ayant répondu au sondage indiquent que les infractions commises contre des systèmes informatiques ou facilitées par l'utilisation d'Internet représentent une part moyenne à élevée de l'ensemble des infractions recensées sur leur territoire. Il faut en effet noter que la cybercriminalité représente plus de 30 % de toutes les infractions déplorées en Afrique de l'Ouest et en Afrique de l'Est, ce qui en fait une préoccupation majeure dans ces sous-régions :

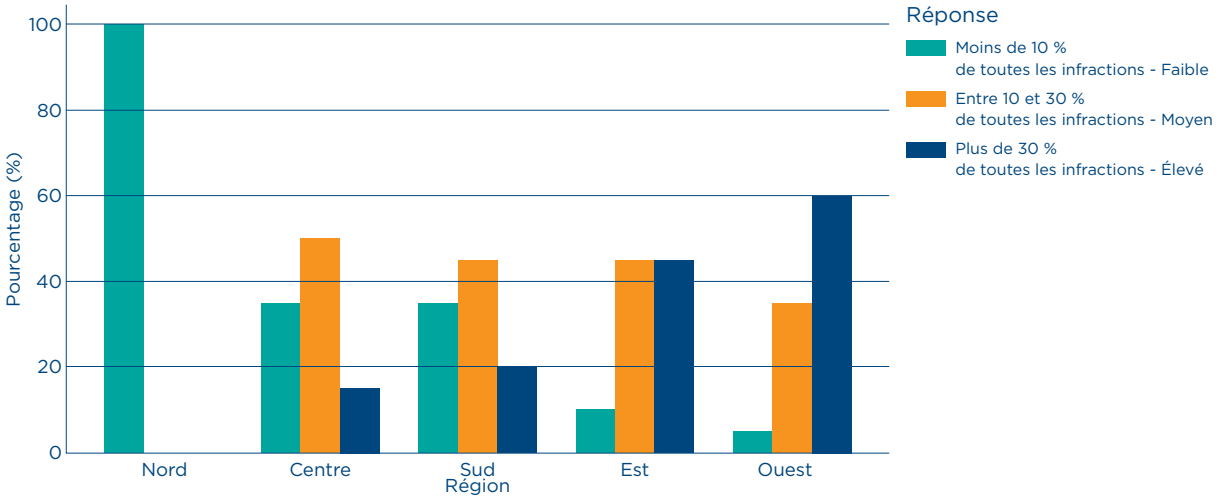


Figure 1. Perception du niveau de risque associé à la cybercriminalité dans les sous-régions d'Afrique selon le sondage réalisé par INTERPOL en 2025 auprès de ses pays membres en Afrique

1 GSMA, L'économie du mobile en Afrique subsaharienne 2024 : https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/12/GSMA_ME_SSA_2024_French.pdf

2 https://innovation-village.com/cybersecurity-in-africa-emerging-threats-and-solutions

3 GSMA, L'économie du mobile en Afrique subsaharienne 2024 : https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/12/GSMA_ME_SSA_2024_French.pdf

4 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

5 Check Point, The State of Cyber Security 2025: https://www.checkpoint.com/security-report

6 https://it-online.co.za/2024/09/13/africa-faces-urgent-cybersecurity-challenges

Les éditions précédentes du rapport citaient les attaques par rançongiciel, les chevaux de Troie bancaires, les voleurs d'informations, les escroqueries en ligne, l'hameçonnage, les escroqueries aux faux ordres de virement (FOVI) et les logiciels malveillants proposés en tant que service, tels que les logiciels espions et les kits d'hameçonnage, comme les cybermenaces les plus répandues[7]. Les escroqueries en ligne, en particulier par hameçonnage, continue d'être les cyberinfractions les plus fréquemment signalées dans les pays membres d'INTERPOL. Les rançongiciels et les FOVI abondent eux aussi. En outre, la sextorsion numérique et l'usurpation d'identité constituent d'autres cybermenaces majeures pour les pays membres en Afrique.

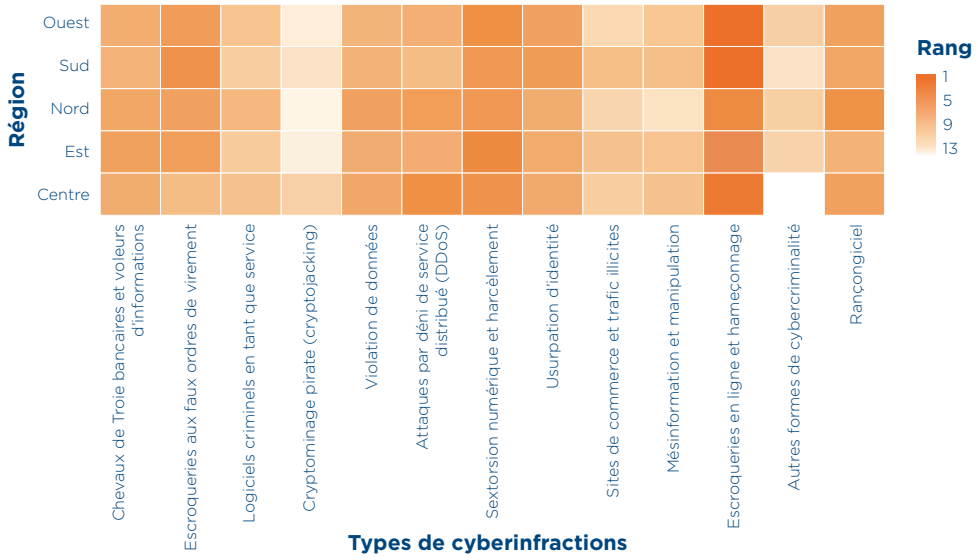


Figure 2. Cybermenaces les plus fréquemment signalées en 2024 par les pays membres d'INTERPOL en Afrique, d'après les résultats du sondage effectué auprès des services chargés de l'application de la loi

Le nombre d'incidents signalés liés aux chevaux de Troie bancaires, aux voleurs d'informations et à la cybercriminalité en tant que service (CaaS) a diminué par rapport aux années précédentes. Cette tendance peut avoir trois explications : une amélioration des interventions des services chargés de l'application de la loi, une plus grande sensibilisation à la cybersécurité, ou une évolution des tactiques des malfaiteurs, qui se tournent dorénavant vers des méthodes plus efficaces telles que la manipulation psychosociale et les escroqueries portées par l'IA.

De nombreux pays membres d'INTERPOL dans la région Afrique font état de répercussions de plus en plus lourdes de la cybercriminalité sur les plans financier et opérationnel. Dans toutes les sous-régions du continent, les escroqueries en ligne, les FOVI, les rançongiciels et les attaques par déni de service distribué (DDoS) sont citées comme les plus préjudiciables d'un point de vue financier. Entre 2019 et 2025, les cyberincidents survenus sur l'ensemble du continent ont entraîné des pertes financières estimées à plus de 3 milliards d'USD[8], les secteurs de la finance, de la santé, de l'énergie et des administrations publiques étant parmi les plus touchés[9]. Ces secteurs stratégiques sont des cibles de choix pour les cyberescrocs, qui en perturbent le fonctionnement et dérobent des données, avec pour corollaire des répercussions financières considérables.

7 Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique : https://www.interpol.int/fr/content/download/21048/file/Rapport-d%27evaluation-des-cybermenaces-en-Afrique.pdf

8 https://african.business/2025/02/apo-newsfeed/over-half-of-africans-fear-financial-losses-from-cybercrime-survey-finds

9 Group-IB, Hi-Tech Crime Trends Report 2023/2024; Middle East & Africa Cyberthreat Landscape : https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

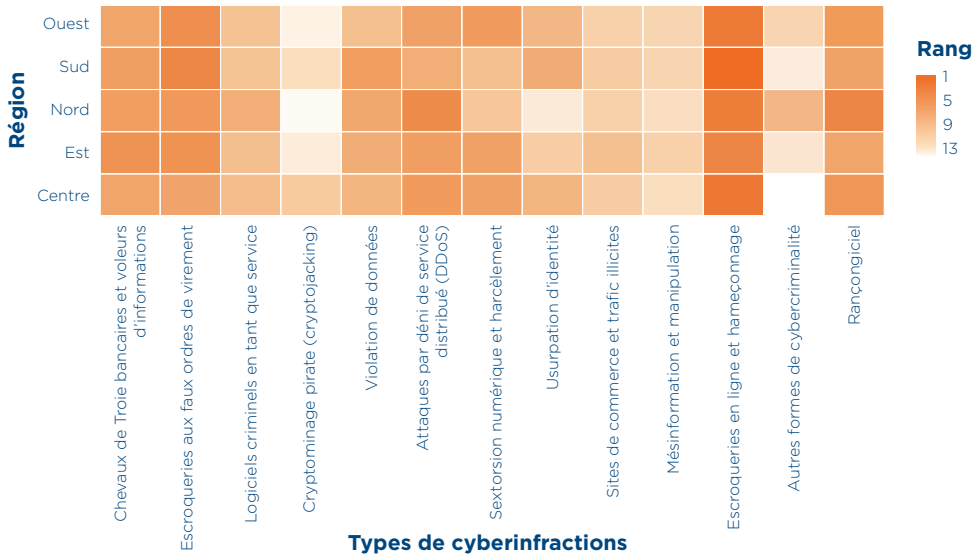


Figure 3. Classement global des types de cybercriminalité selon leur incidence financière déclarée dans les différentes sous-régions africaines, d'après les données fournies par les pays membres d'INTERPOL

Comme signalé par les pays membres d'INTERPOL en Afrique, les cybermalfaiteurs affinent sans cesse leurs tactiques, utilisant des techniques de manipulation psychosociale, l'intelligence artificielle et les plateformes de messagerie instantanée pour lancer des attaques de plus en plus poussées. Les réseaux cybercriminels nationaux et internationaux cherchent souvent à tirer parti des points faibles des individus, en recourant à des supercheries sophistiquées pour cibler les organisations et les particuliers.

2.1 Les cybermenaces les plus répandues en Afrique en 2024

Les résultats du dernier sondage effectué auprès des pays membres africains d'INTERPOL, combinés aux informations fournies par des partenaires du secteur privé[10] et aux conclusions des rapports régionaux sur la cybersécurité, énumèrent comme principales cybermenaces les escroqueries en ligne, les rançongiciels, les FOVI et la sextorsion numérique. Cette section présente une analyse détaillée de l'évolution des cybermenaces en Afrique, en mettant en évidence les plus répandues sur le continent en 2024.

2.1.1. ESCROQUERIES EN LIGNE

Les escroqueries en ligne se multiplient à l'heure actuelle dans plusieurs pays, à mesure que les malfaiteurs du cyberespace adaptent leurs stratagèmes pour frapper là où le bât blesse et tromper aussi bien les particuliers que les entreprises. Les activités frauduleuses, notamment l'hameçonnage et les escroqueries aux sentiments, sont de plus en plus élaborées, moyennant un recours ingénieux à l'intelligence artificielle, à des techniques de manipulation psychosociale et à des manèges sur les réseaux sociaux. Les pays membres d'INTERPOL ont indiqué que ces escroqueries en ligne figuraient parmi les cybermenaces les plus graves auxquelles l'Afrique a été confrontée en 2024, en raison de leur propagation et de leurs répercussions majeures. D'autres sources, notamment des renseignements fournis par des partenaires d'INTERPOL issus du secteur privé, viennent corroborer ce constat.

10 Données transmises par quatre partenaires d'INTERPOL dans le secteur privé, à savoir : Group-IB, Trend Micro, Kaspersky et Bi.Zone.

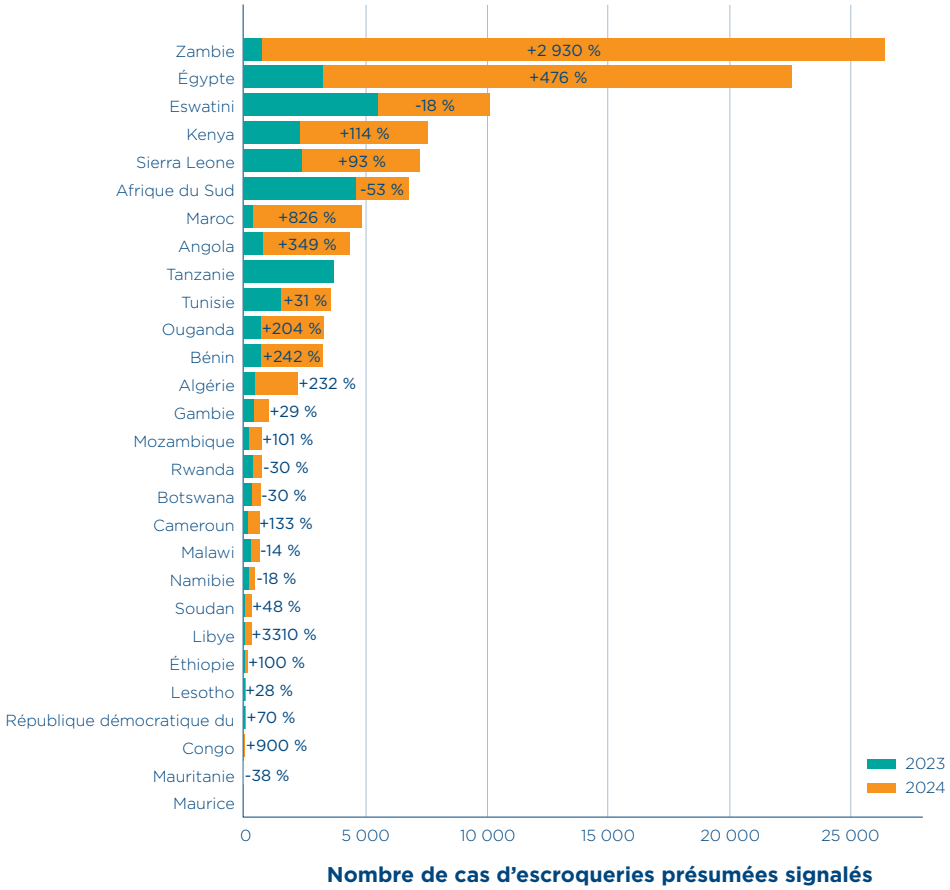


Figure 4. Augmentation des cas d'escroqueries signalés dans les régions africaines entre 2023 et 2024, d'après les données fournies par Kaspersky

L'essor des escroqueries en ligne est étroitement lié à l'accélération de la transformation numérique en Afrique[11]. Les malfaiteurs tirent parti du foisonnement d'activités en ligne, en particulier de l'utilisation des réseaux sociaux, du commerce électronique et des services bancaires mobiles, pour se livrer à leurs exactions. Les données fournies par les pays membres africains d'INTERPOL révèlent que ces escroqueries touchent une population très large : en sont en effet victimes des hommes et des femmes de tous âges et de tous horizons professionnels. Même si les résultats du sondage effectué dans les pays membres soulignent que certains groupes démographiques sont plus vulnérables que d'autres, il apparaît clairement que personne n'est à l'abri du risque.

Les escroqueries en ligne, via l'hameçonnage, restent la cybermenace la plus répandue en Afrique en 2024, touchant à la fois les particuliers et les organisations dans l'ensemble du continent. Les pays membres d'INTERPOL ont placé l'hameçonnage en tête de liste de leurs préoccupations pour la cybersécurité, en raison de son ampleur et de sa récurrence. Selon les rapports sur la sécurité numérique, l'hameçonnage représente 34 % de tous les incidents cybernétiques détectés en Afrique[12]. Les malfaiteurs adeptes de ce stratagème se font passer pour des entités de confiance via des courriels, des plateformes de messagerie ou des sites Web frauduleux, en vue d'inciter les individus à leur dévoiler des informations sensibles telles que leurs identifiants de connexion, leurs données bancaires ou les données de leurs documents d'identité[13]. Une fois obtenus, ces renseignements facilitent les accès non autorisés aux comptes, l'usurpation d'identité et les escroqueries financières. Face à ces méthodes d'hameçonnage de plus en plus sophistiquées, certaines filières essentielles sont aujourd'hui particulièrement vulnérables. C'est notamment le cas du secteur bancaire, des institutions publiques et du secteur des télécommunications.

11 GSMA, L'économie du mobile en Afrique subsaharienne 2024 : https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/12/GSMA_ME_SSA_2024_French.pdf

12 ESET Threat Report : https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf

13 Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique : https://www.interpol.int/fr/content/download/21048/file/Rapport-d%27evaluation-des-cybermenaces-en-Afrique.pdf

Les résultats du sondage d'INTERPOL témoignent d'une évolution notable des tactiques d'hameçonnage, qui deviennent de plus en plus personnalisées, localisées et poussées sur le plan technologique. Les escroqueries habituelles par envoi de courriels en masse ont ainsi fait place à des attaques plus ciblées reposant sur des techniques de manipulation psychosociale. Les cybermalfaiteurs usurpent désormais régulièrement l'identité d'institutions publiques et d'entreprises de renom, font miroiter aux nombreux chômeurs de fausses offres d'emploi et se servent des plateformes en ligne pour échafauder des stratagèmes frauduleux reposant sur de fausses promesses de gains ou de soi-disant situations d'urgence. Par ailleurs, les méthodes d'hameçonnage par SMS (« smishing »), d'hameçonnage téléphonique (« vishing ») et d'hameçonnage via les réseaux sociaux abusent de la confiance des victimes et jouent sur la corde sensible pour les faire tomber dans le piège, ce qui élargit encore plus le spectre des risques[14]. La facilité avec laquelle il est possible de se procurer des outils d'hameçonnage à un prix abordable sur des sites de vente en ligne illicites contribue largement à la prolifération de tels stratagèmes. De plus, pour accroître leur crédibilité et leur force de persuasion, les cybermalfaiteurs s'efforcent d'intégrer dans leurs attaques par hameçonnage des textes, des sons et des vidéos générés par IA, et d'adapter leurs messages aux langues locales et aux contextes culturels[15].

Les informations fournies par les pays membres africains d'INTERPOL ont également souligné à quel point l'hameçonnage est répandu en Afrique et touche de nombreux secteurs, chacun ayant ses propres points faibles et en subissant des conséquences distinctes. Ainsi, les institutions financières connaissent des pertes considérables à cause des vols d'identifiants de connexion et des transactions non autorisées, qui sapent la confiance des consommateurs et freinent l'inclusion numérique dans le secteur bancaire. Les sociétés de télécommunications sont quant à elles confrontées à des problèmes liés à l'exploitation de leur image de marque, aux fraudes par clonage de carte SIM et aux escroqueries par SMS envoyés en masse, qui nuisent à leur réputation et à leur efficacité opérationnelle. Enfin, les gouvernements, les établissements de santé et les centres d'enseignement doivent composer avec des atteintes aux données personnelles des citoyens, des perturbations dans leur fonctionnement et une méfiance croissante du public. Devant un tel constat, il est nécessaire de mettre en place des stratégies d'atténuation des risques à la fois solides et spécifiques à chaque secteur.

En 2024, les escroqueries aux sentiments se sont multipliées en Afrique, devenant l'une des escroqueries en ligne les plus courantes sur le continent. Éperonnés par l'essor de l'accès à Internet et la généralisation des réseaux sociaux, les fraudeurs ont recours à des tactiques de plus en plus élaborées et préjudiciables. D'après les données fournies par les pays membres d'INTERPOL, les malfaiteurs abordent le plus souvent leurs cibles via les réseaux sociaux, les services de messagerie et les applications de rencontre en ligne. Ils cherchent à nouer un lien personnel avec leurs victimes en jouant sur leurs points faibles. Cette démarche peut aller d'échanges très brefs à un dialogue prolongé s'étendant sur plusieurs années. Une fois la confiance établie, ils manipulent leurs victimes pour faire en sorte que celles-ci leur remettent de l'argent ou d'autres biens.
Les escroqueries aux sentiments sont un problème très répandu en Afrique, en particulier dans certaines régions. Ainsi, les pays d'Afrique de l'Ouest, notamment le Nigéria, le Ghana, la Côte d'Ivoire et le Bénin, recensent des réseaux particulièrement actifs se livrant à ce type d'escroqueries[16]. Une nouvelle tendance a récemment vu le jour dans la région : les malfaiteurs bernent leurs victimes à base de promesses sentimentales, puis les contraignent à investir de l'argent dans des systèmes de cryptomonnaie frauduleux[17].

À l'origine de préjudices émotionnels et financiers considérables, les escroqueries aux sentiments sont de nos jours des formes très lucratives de cybercriminalité. Dans une affaire retentissante au Nigéria, un seul escroc est parvenu à soutirer plus de 1,9 million d'USD à ces nombreuses victimes avant d'être arrêté[18]. Les données d'INTERPOL font état de nombreux cas dans lesquels des victimes africaines ont versé à plusieurs reprises de l'argent à des escrocs, parfois au point d'épuiser leurs fonds de retraite ou de s'endetter. Or, il n'est pas rare que les victimes passent leur déconvenue sous silence, en raison de la honte et de la culpabilité qu'elles ressentent, ou par peur d'être stigmatisées. Il est donc probable que l'incidence financière réelle de ces escroqueries soit bien plus importante que les chiffres officiellement consignés[19]. Compte tenu de la complexité et de l'ampleur croissantes de ces méfaits, il est urgent d'organiser des formations spécialisées dans les services chargés de l'application de la loi des pays africains et de renforcer leurs capacités en matière de criminalistique afin de lutter efficacement contre ces menaces grandissantes et d'enquêter à leur sujet.

14 https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase

15 https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime

16 https://theconversation.com/online-romance-scams-who-nigeria-and-ghanas-fraudsters-are-how-they-operate-and-why-they-do-it-247916

17 https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16/

18 https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/Des-cybermalfaiteurs-arretes-lors-d-une-operation-internationale-en-Afrique-de-l-Ouest

19 https://www.knowbe4.com/hubfs/Online-Scams+Victims-Africa-report-2024.pdf

2.1.2. RANÇONGICIELS

Représentant un risque de plus en plus présent dans les administrations, les entreprises et les services essentiels, les rançongiciels ont été cités par les pays membres d'INTERPOL comme l'une des cybermenaces les plus répandues sur le continent africain en 2024. D'après les données des partenaires d'INTERPOL dans le secteur privé, le nombre de cas de rançongiciels recensés chaque mois en Afrique a augmenté en 2024 par rapport à l'année précédente[20]. Ces attaques sont particulièrement préoccupantes en raison de leurs grandes répercussions financières, de leur capacité à perturber gravement le fonctionnement des infrastructures critiques et des préjudices qu'elles causent aux organisations et aux personnes qui en sont victimes. Selon des rapports publiés par des sociétés de cybersécurité[21] et des partenaires d'INTERPOL dans le secteur privé, l'Afrique du Sud et l'Égypte ont connu le plus grand nombre d'incidents liés à des rançongiciels en 2024, suivis par d'autres pays dont l'économie repose en grande partie sur le numérique, tels que le Nigéria, le Kenya, la Gambie, la Tunisie et le Maroc. L'Algérie, l'Éthiopie et même des États plus petits comme le Bénin ont également déclaré avoir subi des attaques importantes. Les rançongiciels constituent donc un défi de taille à l'échelle du continent, en particulier dans les pays dotés d'une infrastructure numérique plus développée.

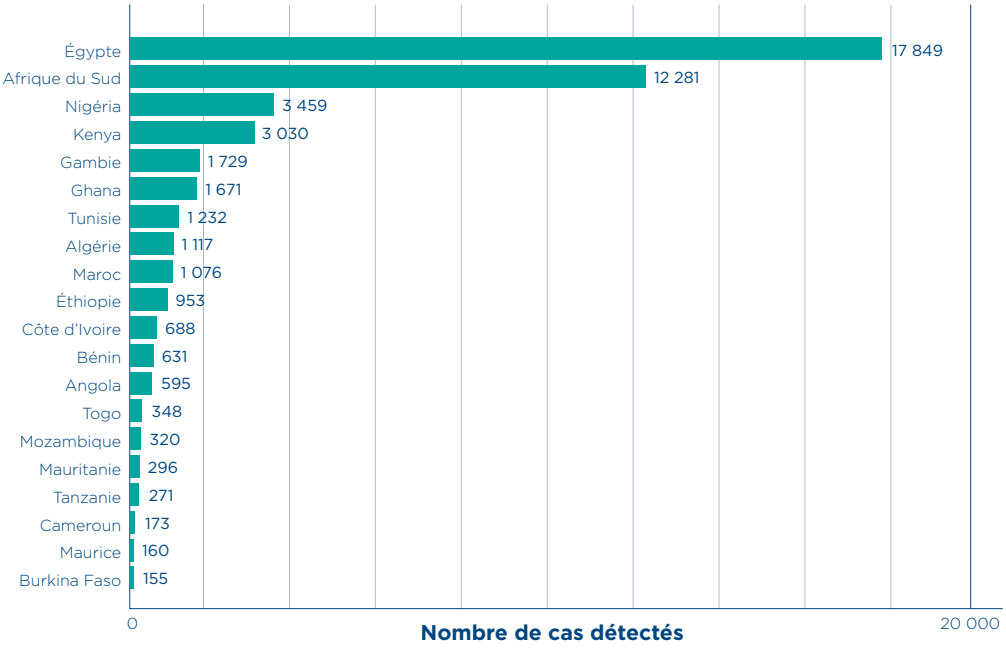


Figure 5. Classement des 20 pays africains ayant détecté le plus grand nombre de cas de rançongiciels en 2024, selon les données de Trend Micro.

Les rançongiciels ont entraîné des répercussions financières colossales en Afrique en 2024. Certains incidents consistaient en des vols purs et simples, comme le cyberbraquage de la société nigériane de technologie financière Flutterwave en avril, qui aurait permis aux malfaiteurs de détourner près de 7 millions d'USD[22]. Dans d'autres cas, les demandes de rançon allaient de plusieurs dizaines de milliers à plusieurs millions de dollars, des sommes souvent exigées en cryptomonnaie qui représentaient des préjudices financiers considérables. De plus, les perturbations causées par les rançongiciels ont provoqué l'interruption d'activités commerciales assortie d'un manque à gagner et d'une baisse de productivité, ainsi que des frais de rétablissement conséquents.

20 D'après les données fournies par Trend Micro, 2024.

21 https://falconfeeds.io/blogs/cyber-attacks-in-africa-a-comprehensive-analysis-of-trends-from-january-to-august-2024-206317

22 https://africa.businessinsider.com/local/markets/fintech-giant-flutterwave-loses-naira11-billion-to-security-breach

La compagnie d'électricité du Cameroun (ENEO) a été contrainte d'interrompre ses opérations, tandis que l'autorité responsable du réseau routier urbain du Kenya (KURA) a subi une attaque compromettant des données essentielles relatives aux infrastructures routières[23]. Les bases de données des administrations publiques n'ont pas été épargnées non plus, Ainsi, en décembre 2024, des piratages informatiques ont touché l'autorité kenyane responsable des micro et petites entreprises (MSEA) et le Bureau national des statistiques du Nigéria (NBS)[24]. Fin 2024, le ministère sud-africain de la Défense a été victime du groupe de cyberrançonneurs Snatch, qui lui a dérobé 1,6 To de données, y compris le numéro de téléphone et l'adresse électronique personnels du président du pays[25]. Le secteur des télécommunications a lui aussi été confronté à des menaces similaires, comme l'illustre l'attaque perpétrée contre Telecom Namibia fin 2024, au cours de laquelle la confidentialité d'environ 626,3 Go de données, réparties dans plus de 492 000 fichiers, a été compromise, affectant plus de 619 000 clients[26]. Portant atteinte à des informations sensibles appartenant à des particuliers, des entreprises et des organismes publics, cette intrusion a mis en évidence l'existence de risques importants pour la vie privée des citoyens et la sécurité nationale[27].

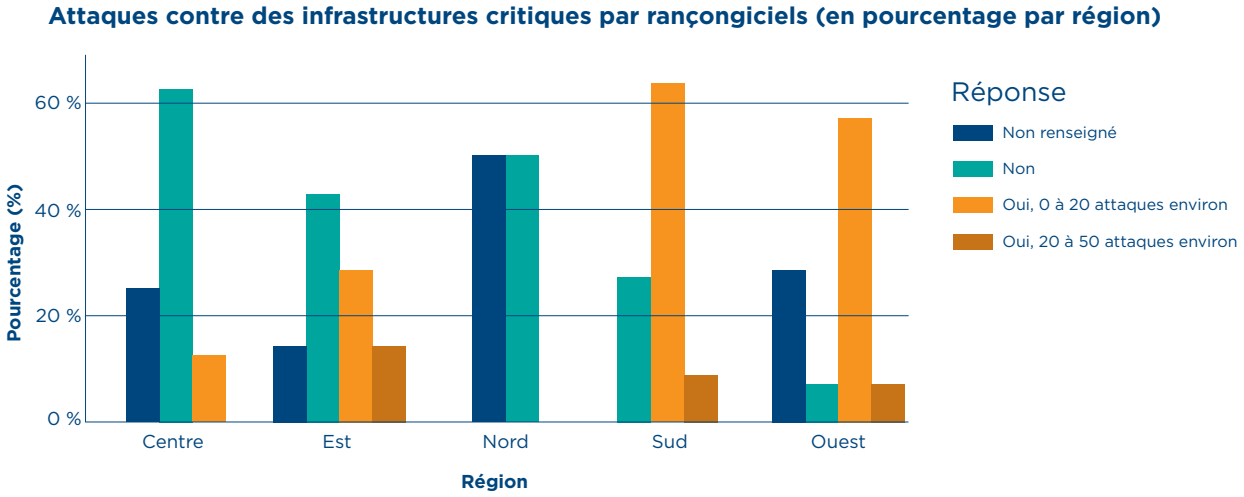


Figure 6. Attaques contre des infrastructures critiques par rançongiciels par région (en %), d'après les réponses au sondage réalisé en 2024 par INTERPOL auprès de ses pays membres en Afrique

Selon les données fournies par les partenaires d'INTERPOL dans le secteur privé[28], plusieurs groupes de pirates informatiques sévissaient dans toute la région Afrique en 2024. L'un des plus importants était LockBit, une bande organisée prolifique dans le domaine des rançongiciels en tant que service (RaaS), qui s'est montrée particulièrement active tout au long de l'année. Connu pour ses méthodes agressives de double extorsion, consistant à crypter les réseaux de ses victimes tout en les menaçant de divulguer leurs données dérobées, LockBit a revendiqué une attaque perpétrée en février contre le Fonds de pension des fonctionnaires sud-africains (GEPF)[29]. De nombreux incidents en Afrique de l'Ouest lui sont également imputés[30]. Bien que les autorités aient temporairement mis hors service les sites de LockBit sur l'Internet clandestin lors d'une opération internationale de lutte contre la cybercriminalité, le groupe a rapidement refait surface pour divulguer ou retransmettre les données de ses victimes, provoquant de graves perturbations et d'importantes violations de données[31]. L'attaque contre le GEPF a touché à elle seule plusieurs millions de personnes, ce qui souligne à quel point la poursuite des activités de LockBit s'avère dangereuse.

23 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
24 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
25 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
26 https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked
27 https://dailysecurityreview.com/news/namibia-ransomware-attack-sensitive-data-of-government-officials-and-citizens-leaked/
28 D'après les données fournies par Bi.Zone, 2024.
29 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
30 https://toptechgh.com/lockbit-ransomware-member-extradited-see-attacks-on-africa
31 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack

Un autre acteur de premier plan dans le domaine des rançongiciels, Hunters International (Hunters), s'en prend tout particulièrement aux télécommunications, aux administrations publiques et aux institutions financières en Afrique[32]. En juillet 2024, Hunters s'est ainsi immiscé dans les services de l'autorité responsable du réseau routier urbain du Kenya (KURA) pour s'emparer de près de 18 Go de données[33]. Il a de nouveau frappé au mois de décembre, en attaquant Telecom Namibia et en divulguant des informations sensibles sur sa clientèle[34]. Hunters applique des méthodes furtives, consistant à extraire discrètement des données avant de crypter les systèmes. À ce stade, les données des victimes qui refusent de payer la rançon sont rendues publiques. Cette tactique entraîne d'importantes perturbations dans le fonctionnement des services et minent la confiance des citoyens. BlackSuit, un groupe de cyberrançonneurs spécialisé dans l'extorsion et connu pour cibler de grandes organisations à l'échelle mondiale, a démontré son manque total de scrupules en s'attaquant aux laboratoires du service national de santé publique (NHLS) d'Afrique du Sud en juin 2024[35]. En conséquence, les diagnostics associés à des millions d'examens médicaux ont été retardés, des opérations chirurgicales vitales ont été annulées et plus d'un téraoctet de données hautement sensibles ont été compromises. Cet incident déplorable illustre parfaitement à quel point les rançongiciels représentent un risque pour la santé et la sécurité de la population.

2.1.3. ESCROQUERIES AUX FAUX ORDRES DE VIREMENT

Les pays membres d'INTERPOL en Afrique ont mentionné les escroqueries aux faux ordres de virement (FOVI) comme une cybermenace importante et en plein essor dans le contexte global des escroqueries en ligne. D'après les données fournies par des partenaires d'INTERPOL dans le secteur privé[36], les activités cybercriminelles liées au FOVI sont en forte hausse dans toute l'Afrique, aussi bien en chiffres absolus qu'en termes de fonds détournés. Un nombre non négligeable d'escrocs spécialisés dans les FOVI opèrent depuis le continent africain, en particulier en Afrique de l'Ouest. Selon les données fournies par ces partenaires du secteur privé, 11 pays africains concentrent la majorité des activités liées aux FOVI émanant du continent, avec en tête le Nigéria, le Ghana, la Côte d'Ivoire et l'Afrique du Sud. En Afrique de l'Ouest, ces escroqueries ont donné des ailes à des réseaux criminels extrêmement organisés devenus multimillionnaires. Comptant des milliers de membres répartis dans le monde entier, le groupe criminel international connu sous le nom de « Black Axe » est à l'origine d'escroqueries financières à grande échelle qui lui ont rapporté des milliards de dollars[37].

D'après les données fournies par les pays membres d'INTERPOL en Afrique, le secteur le plus fréquemment pris pour cible en 2024 sur le continent a été celui de la banque et de la finance. Les entreprises qui exercent des activités à l'international, celles qui effectuent fréquemment des transactions financières et celles qui ne disposent pas de contrôles de sécurité perfectionnés sont particulièrement vulnérables aux FOVI. Il convient cependant de noter qu'aucun secteur n'est à l'abri de ces attaques. En effet, elles touchent des organisations de toutes tailles, aussi bien de petites et moyennes entreprises que de grandes sociétés. Outre les banques et les institutions de microfinancement, des entreprises intervenant dans les secteurs de l'import-export, du pétrole et du gaz, des produits pharmaceutiques, du transport et du commerce électronique ont elles aussi connu des incidents graves. Par ailleurs, les attaques contre les organismes publics, le secteur du bénévolat et les particuliers se sont multipliées sur le continent africain.

Il est difficile d'obtenir des chiffres précis sur le nombre d'incidents réels liés aux FOVI en Afrique dans la mesure où ceux-ci ne sont pas toujours signalés. Toutefois, plusieurs indicateurs révèlent l'ampleur du problème. Pour la seule année 2024, 19 pays africains ont rapporté en tout et pour tout 10 490 arrestations pour des faits relevant de la cybercriminalité. Ces chiffres laissent penser que le nombre de cas de FOVI est en réalité très élevé, étant donné que seulement 35 % des cyberinfractions en moyenne sont officiellement signalées[38]. En novembre 2024, une affaire très médiatisée est venue illustrer la portée mondiale des réseaux cybercriminels africains. Il s'agit de la condamnation, par les autorités américaines, d'un ressortissant nigérian de 33 ans, Babatunde Ayeni, à 10 ans de prison pour avoir orchestré une vaste escroquerie de type FOVI autour de transactions immobilières[39]. À l'œuvre depuis le Nigeria et les Émirats arabes unis, cet escroc et ses complices avaient recours à l'hameçonnage pour voler les identifiants de connexion de notaires et d'agents immobiliers aux États-Unis leur permettant d'accéder à leurs comptes de messagerie électronique. Ils usurpaient ensuite l'identité de ces professionnels dans le but de rediriger les paiements associés au remboursement de prêts hypothécaires vers des comptes frauduleux. Plus de 400 personnes ont fait les frais de ce stratagème, qui a permis aux escrocs de détourner 19,6 millions d'USD et de les transférer vers des comptes dont ils avaient le contrôle[40]. Cette affaire a mis en évidence que les FOVI revêtent un caractère international, tout en montrant comment les réseaux cybercriminels africains exploitent les systèmes financiers mondiaux pour flouer leurs victimes partout dans le monde.

32 D'après les données fournies par Bi.Zone, 2024.

33 https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia

34 https://magedata.ai/securefact/securefact-cyber-security-news-week-of-december-23-2024

35 https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa

36 D'après les données fournies par Trend Micro, 2024.

37 https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime

38 https://therecord.media/orion-carbon-black-bec-scam-millions

29 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme

40 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme

En ce qui concerne les modes opératoires, les données provenant des pays membres d'INTERPOL en Afrique indiquent que les escroqueries aux FOVI commises dans l'ensemble du continent s'appuient sur la manipulation psychosociale, l'hameçonnage, l'usurpation d'identité et l'intrusion dans les réseaux pour détourner les transactions financières. Une tactique couramment employée par les cybermalfaiteurs consiste à se faire passer pour des cadres dirigeants, des partenaires commerciaux ou des fonctionnaires en vue de berner les employés d'une organisation et les inciter à transférer des fonds. Les « escroqueries au président » et les fraudes au changement de coordonnées bancaires, en particulier dans le secteur public, figurent parmi les subterfuges les plus couramment employés. L'hameçonnage et le vol d'identifiants de connexion sont amplement utilisés pour accéder à des comptes. Certains pirates n'hésitent pas à recourir à la manipulation psychosociale via WhatsApp en se faisant passer pour des contacts connus de la victime. Des cas encore plus élaborés reposent sur une intrusion dans un réseau, pour y déployer des logiciels malveillants afin de surveiller les échanges de courriels et d'intercepter les processus de paiement. En Afrique de l'Ouest et en Afrique australe, les malfaiteurs ont souvent recours à des « sosies » de domaines ou à des adresses électroniques légèrement modifiées pour leurrer leurs victimes. Les escroqueries liées aux devis et aux paiements sont également monnaie courante : les malfaiteurs envoient des demandes de devis frauduleuses ou invoquent un changement de coordonnées bancaires.

Les rapports des pays membres d'INTERPOL révèlent par ailleurs que la cybercriminalité en tant que service (CaaS) contribue à la sophistication croissante des attaques de type FOVI. Le service de Microsoft chargé de la lutte contre la criminalité numérique a détecté une augmentation de 38 % de la CaaS visant les comptes de messagerie professionnels entre 2019 et 2022[41]. Désormais, les cybermalfaiteurs ont accès à des kits d'hameçonnage prêts à l'emploi, qui leur permettent d'accomplir leurs desseins plus efficacement et à grande échelle. Les plateformes illicites telles que BulletProofLink facilitent encore davantage les campagnes de FOVI de grande ampleur en proposant des services complets, notamment d'hébergement et d'automatisation, ainsi que des modèles à reproduire[42]. Ces plateformes aident également les malfaiteurs à contourner les mesures de sécurité telles que les alertes de type « Impossible Travel », en utilisant des adresses IP résidentielles.

Par ailleurs, les FOVI portées par l'IA constituent une nouvelle menace à ne pas négliger. INTERPOL a publié une notice mauve mettant en garde contre les malfaiteurs qui se servent de l'intelligence artificielle et de l'hypertrucage à mauvais escient pour perfectionner leurs escroqueries[43]. L'IA générative leur permet en effet de rédiger des courriels personnalisés très convaincants, qui imitent le style et le vocabulaire d'une organisation ou d'une personne donnée. Quant à l'hypertrucage, il s'agit d'une technologie d'ores et déjà utilisée pour usurper l'identité de cadres supérieurs lors d'appels téléphoniques ou vidéo. L'évolution rapide de l'IA pose un risque important, en ce qu'elle permet la propagation des attaques de type FOVI et leur confère davantage de crédibilité. Les pays membres doivent donc rester aux aguets.

2.1.4. Sextorsion numérique

La sextorsion numérique est un type d'Abus Sexuel En ligne Basé sur l'Image (ASEBI) dans laquelle les auteurs de menaces utilisent des images sexuellement explicites pour extorquer leurs victimes en les menaçant de divulguer ces images sans leur consentement. Ces images sont parfois authentiques, quand elles ont été fournies volontairement ou obtenues par la contrainte ou la duperie, parfois générées par intelligence artificielle ou manipulées par des outils numériques[44]. La sextorsion répond généralement à des motifs d'ordre financier. Toutefois, elle peut aussi être motivée par un désir de vengeance ou de coercition.

Les ASEBI, et la sextorsion en particulier, sont des formes de cybercriminalité en plein essor dans l'Afrique de 2024. En effet, d'après les données fournies par les pays africains membres d'INTERPOL, les signalements de cas de sextorsion numérique ont considérablement augmenté, plus de 60 % de ces pays déclarant avoir constaté une telle hausse. Il est probable que cette tendance ne soit que la pointe de l'iceberg en ce qui concerne l'évolution du panorama numérique dans la région. En effet, compte tenu du nombre important de cas non signalés, en particulier pour les infractions de cette nature, l'ampleur réelle de ce phénomène est sans doute beaucoup plus importante. Il est important de noter que les données actuellement disponibles ne tiennent pas compte des cas signalés par des victimes situées hors d'Afrique, ce qui porte à croire que ces cybermenaces sont bien plus répandues et imbriquées à l'échelle mondiale que ce que les chiffres régionaux ne laissent entendre.

41 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

42 Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique : https://www.interpol.int/fr/content/download/21048/file/Rapport-d%27evaluation-des-cybermenaces-en-Afrique.pdf

43 Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique : https://www.interpol.int/fr/content/download/21048/file/Rapport-d%27evaluation-des-cybermenaces-en-Afrique.pdf

44 https://www.trendmicro.com/vinfo/sg/security/definition/digital-extortion

Les mesures prises récemment par les principales plateformes de réseaux sociaux témoignent de l'ampleur grandissante des ASEBI. Au milieu de l'année 2024, Meta a supprimé plus de 63 000 comptes Instagram et 7 000 entités Facebook liés à des cas de sextorsion numérique au Nigéria[45] [46]. Bien que l'on ignore à quel moment ces comptes ont été repérés, l'ampleur de l'opération suggère soit une montée en puissance des activités malveillantes, soit une pression externe croissante sur les plateformes pour qu'elles réagissent. Quoi qu'il en soit, ces deux indicateurs sont révélateurs d'une augmentation de la criminalité. Bon nombre de ces comptes étaient liés à des réseaux cybercriminels organisés, dont certains contribuaient au recrutement et à la formation de cyberdélinquants, ainsi qu'à la distribution de manuels opérationnels pour apprendre à commettre des infractions numériques à caractère sexuel[47] [48]. Cela dénote une évolution tactique : le chantage sexuel n'est plus seulement utilisé comme moyen de pression isolé, mais comme faisant partie des tactiques, techniques et procédures (TTP) récurrentes au sein des systèmes traditionnels d'escroquerie. Certains indices suggèrent par ailleurs que ces réseaux pourraient rejoindre ceux de groupes criminels organisés établis de longue date en Afrique de l'Ouest, mais cette piste reste à confirmer[49].

Parallèlement à l'évolution des menaces en termes d'ampleur et de perfectionnement, de nouveaux vecteurs de risque ont fait leur apparition. Les partenaires d'INTERPOL dans le secteur privé signalent une forte augmentation des courriels d'hameçonnage utilisés pour lancer des campagnes de sextorsion[50]. En outre, on constate une multiplication des stratagèmes d'extorsion assistés par l'IA, dans lesquels des images explicites, synthétiques ou modifiées, sont utilisées pour tromper les victimes. Le Maroc, le Mali, l'Égypte et la Mauritanie sont les pays qui ont enregistré le nombre le plus élevé d'incidents de ce type, soulignant leur répartition dans la région. Cette convergence entre l'hameçonnage, les outils d'intelligence artificielle et les artifices tactiques dénote une systématisation de la sextorsion. Ainsi, celle-ci n'est plus seulement l'œuvre de malfaiteurs opportunistes ; elle s'intègre progressivement dans des structures de fraude plus larges.

Bien que la plupart des victimes des activités liées aux ASEBI sur les plateformes Meta soient des adultes, les services chargés de l'application de la loi ont signalé une augmentation inquiétante du nombre de cas touchant des adolescents et adolescentes, y compris en dehors de l'Afrique[51, 52]. Cette baisse apparente de l'âge des victimes, couplé à l'amplitude géographique croissante des escroqueries, pourraient indiquer un changement de stratégie. Cela soulève également des questions de fond concernant les motivations qui sous-tendent la sextorsion numérique. Si l'objectif principal reste le chantage économique, consistant généralement à menacer de diffuser des images sexuellement explicites, certains incidents suggèrent des motivations davantage fondées sur la manipulation psychologique, la coercition ou l'intention de nuire à la réputation des victimes. Dans de tels cas, les malfaiteurs seraient plus enclins à tirer parti des points faibles des individus pour les contrôler plutôt que pour leur soutirer de l'argent. Pour les victimes, le préjudice psychologique est considérable. En Afrique du Sud, les autorités ont signalé une augmentation du nombre de victimes chez les adolescents, et un adulte s'est suicidé à la suite d'un cas de sextorsion[53]. En Égypte, une plateforme d'assistance numérique a reçu plus de 250 000 appels liés à la sextorsion en 2024, principalement de la part de femmes et de filles[54, 55] . Ces chiffres sont le miroir d'une crise invisible mais généralisée, où la peur, la stigmatisation et la détresse émotionnelle sont systématiquement mises à profit par les auteurs de menaces dans le cadre de leur tactique de contrôle.

Les services chargés de l'application de la loi en Afrique ont redoublé d'efforts face à cette menace grandissante, notamment en renforçant la coordination internationale, la coopération transfrontalière et la collaboration avec les plateformes du secteur privé. Cependant, un manque de moyens persistant, des problèmes de compétence juridique et des délais dans l'accès aux données d'autres pays continuent de freiner les enquêtes. Étant donné que les malfaiteurs ne connaissent pas de frontières et que leurs victimes sont réparties dans plusieurs pays, les cadres d'application de la loi existants ont du mal à s'adapter à la nouvelle donne.

45 https://www.npr.org/2024/07/24/nx-s1-5050709/meta-sextortion-scams-nigeria-facebook-instagram
46 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
47 https://tuxcare.com/blog/sextortion-scams-63k-instagram-account-in-nigeria-removed
48 https://www.theverge.com/2024/7/24/24205236/meta-nigeria-financial-sextortion-scam
49 https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf
50 D'après les données fournies par Trend Micro, 2024.
51 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
52 https://businesstech.co.za/news/internet/790431/extortion-syndicates-targeting-boys-in-south-africa
53 https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion
54 https://allafrica.com/stories/202408190082.html
55 https://www.reuters.com/article/technology/feature-egyptian-women-find-help-online-to-fight-sextortion-threats

3. TENDANCES DES CYBER-MENACES ET PERSPECTIVES DANS LES SOUS-RÉGIONS AFRICAINES

Sur l'ensemble du continent africain, les tendances en matière de cybermenaces suivent généralement des schémas similaires ; les escroqueries en ligne, les rançongiciels, les escroqueries aux faux ordres de virement (FOVI) et la sextorsion numérique y figurent parmi les plus graves. Cependant, la nature et l'ampleur de ces menaces varient d'une sous-région à l'autre en raison des décalages existants en ce qui concerne l'infrastructure numérique, les moyens à la disposition des services chargés de l'application de la loi et les tactiques utilisées par les cybermalfaiteurs. Cette section passe en revue les tendances régionales de la cybercriminalité et son évolution en Afrique de l'Ouest, en Afrique de l'Est, en Afrique centrale, en Afrique australe et en Afrique du Nord, et décrit la manière dont elle se manifeste dans chacune de ces sous-régions.

3.1 Afrique de l'Ouest

- Le Nigéria, le Ghana, la Côte d'Ivoire et le Sénégal contribuent de manière prépondérante à l'économie numérique et à l'activité cybernétique de l'Afrique de l'Ouest[56]. • Ces pays ne sont pas seulement des plaques tournantes de l'innovation technologique et des centres de services financiers, mais constituent également des cibles privilégiées pour les malfaiteurs à l'œuvre dans le cyberespace, dont les menaces remodèlent l'écosystème global de la région en matière de cybersécurité.
- Les FOVI figurent toujours parmi les cybermenaces les plus préjudiciables sur le plan économique, avec des groupes basés en Afrique de l'Ouest qui ciblent des entreprises du monde entier.
- Les attaques par rançongiciel représentent elles aussi une cybermenace de premier plan. Leurs auteurs, en particulier ceux qui opèrent selon le modèle de rançongiciel en tant que service (RaaS), se servent d'organisations africaines comme bancs d'essai pour tester de nouveaux logiciels malveillants[57]. Ces attaques s'inscrivent généralement dans un modèle de double extorsion, consistant à chiffrer les données des victimes tout en les menaçant de divulguer leurs informations sensibles si elles refusent de payer la rançon exigée.
- Les attaques par déni de service distribué (DDoS) restent une préoccupation majeure dans la région. Au cours du premier semestre 2024, le Ghana a recensé 4 753 cas de DDoS, avec des pics d'attaques atteignant 314 gigaoctets par seconde (Gbps), ce qui en a fait l'une des principales cibles de DDoS en Afrique[58].
- La fraude liée aux portefeuilles mobiles est en forte hausse. Les escrocs utilisent des techniques de manipulation psychosociale pour pirater des comptes et demander de l'argent en urgence à des contacts peu méfiants. Les escroqueries liées aux services de paiement par téléphone mobile, notamment les fraudes par clonage de carte SIM et les fraudes aux télécommunications, sont très répandues, tandis que l'usurpation d'identité favorise la multiplication des escroqueries liés aux placements, aux paris et aux achats en ligne.
- En hausse également, l'escroquerie aux sentiments consiste notamment à faire chanter les victimes sous la menace de divulguer des informations sensibles. Depuis peu, les escrocs tendent aussi à séduire leurs victimes avec des promesses d'amour, avant de les contraindre à investir de l'argent dans des systèmes de cryptomonnaie frauduleux.

56 https://arxiv.org/html/2402.01649v1
57 https://www.darkreading.com/cyberattacks-data-breaches/criminals-test-ransomware-africa
58 https://toptechgh.com/ghana-hit-with-4753-ddos-attacks-netscout-threat-intelligence-report-1h-2024

3.2 Afrique de l'Est

- En Afrique de l'Est, progressant considérablement sur la voie de la transformation numérique, le Kenya, l'Ouganda, la Tanzanie, le Rwanda et l'Éthiopie sont en passe de devenir de véritables pôles technologiques et financiers. Cependant, ces progrès les rendent de plus en plus attrayants pour les cyberescrocs, d'où la nécessité urgente de mettre en place de solides mécanismes pour assurer la cybersécurité.
- L'Éthiopie est devenue le pays le plus ciblé au monde par les cyberattaques en 2024, se hissant en tête du classement mondial par nombre de logiciels malveillants détectés[59].
- Les infrastructures critiques, notamment les institutions publiques, les services financiers et les grands projets de développement, sont fréquemment pris pour cible.
- Les fraudes par échange de carte SIM ont considérablement augmenté en Ouganda et en Tanzanie. Les malfaiteurs exploitent les failles des réseaux mobiles en se procurant de manière frauduleuse des cartes SIM de remplacement, souvent par supercherie ou à l'aide de complices initiés, ce qui leur permet d'usurper les numéros de téléphone de leurs victimes.
- La sextorsion numérique est une cybermenace en pleine expansion en Afrique de l'Est. Ciblant surtout les femmes et les jeunes, les malfaiteurs mettent à profit des contenus compromettants pour faire chanter leurs victimes.

3.3 Afrique centrale

- En Afrique centrale, les cyberattaques tirent souvent parti de la faiblesse des infrastructures de protection et de l'obsolescence des systèmes.
- Les escroqueries par manipulation psychosociale figurent parmi les cyberinfractions les plus fréquemment signalées, les criminels utilisant des tactiques insidieuses telles que de fausses offres d'emploi et des escroqueries aux sentiments pour attirer des victimes ingénues dans leurs pièges.
- Les institutions bancaires et financières sont de plus en plus exposées aux escroqueries aux faux ordres de virement (FOVI) et aux intrusions dans leurs réseaux. Le Cameroun et le Gabon ont signalé une augmentation notable des cyberattaques visant leurs institutions financières, entraînant des pertes considérables.

3.4 Afrique australe

- L'Afrique australe est réputée posséder l'un des écosystèmes de cybersécurité les plus avancés du continent. Des pays comme l'Afrique du Sud, la Namibie et le Botswana investissent amplement dans la sensibilisation à la cybersécurité, dans des cadres juridiques complets et dans des technologies de sécurité fondées sur l'IA.
- Les malfaiteurs ont adopté des outils reposant sur l'IA pour créer des hypertrucages perfectionnés imitant des voix et des images vidéo, afin de se faire passer pour des PDG ou des fournisseurs. En 2024, le nombre d'attaques de ce type par hameçonnage vocal est ainsi grimpé en flèche[60].
- La manipulation psychosociale demeure une méthode très répandue et sert souvent de tremplin pour lancer des attaques. Ciblant particulièrement les clients des banques, l'hameçonnage par SMS (« smishing ») repose sur des messages trompeurs, conçus pour permettre aux malfaiteurs d'accéder aux comptes des utilisateurs.
- Les cyberescrocs d'Afrique australe tirent de plus en plus parti des nouvelles tendances en matière de technologies financières, notamment des services bancaires numériques et des cryptomonnaies. Ainsi, la tactique du cryptominage pirate (« cryptojacking ») se répand progressivement, les institutions financières ayant signalé une augmentation considérable du nombre d'incidents de ce type en 2024.

59 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024/

60 https://qtatech.com/en/article/why-are-cyberattacks-increasingly-targeting-african-financial-institutions?srsltid=AfmBOoqghmt5QRlVko-UqiSdks8zjt99y1nHYR24zzh1vf63gxMYTk2a

3.5 Afrique du Nord

- En Afrique du Nord, l'Égypte, l'Algérie, le Maroc, la Tunisie et la Libye ont tous été confrontés en 2024 à un ensemble de cybermenaces de plus en plus perfectionnées, influencées par les tendances mondiales en matière de cybercriminalité et le contexte géopolitique régional.
- De fait, l'Égypte et le Maroc figuraient parmi les pays les plus touchés d'Afrique en raison de l'utilisation très répandue d'Internet sur leur territoire et du poids de leur économie. Ainsi, l'Égypte a recensé à elle seule près de 13 % de toutes les cyberattaques perpétrées sur le continent en 2024, se classant au deuxième rang derrière l'Afrique du Sud[61].
- La manipulation psychosociale continue d'être à l'origine de nombreux incidents cybernétiques en Afrique du Nord, allant des escroqueries les plus simples à des attaques hautement sophistiquées. Les entreprises ont souvent été la cible de courriels d'hameçonnage personnalisés et rédigés dans la langue locale afin d'en accroître la crédibilité. Les escroqueries liées aux loteries et aux placements en ligne sont elles aussi monnaie courante. Ainsi, de nombreux incidents ont été signalés dans lesquels les malfaiteurs envoyaient des messages via WhatsApp promettant de faux prix ou des opportunités d'investissement frauduleuses dans les cryptomonnaies.

AFRIQUE CENTRALE	AFRIQUE DE L'EST	AFRIQUE DU NORD	AFRIQUE AUSTRALE	AFRIQUE DE L'OUEST
Le manque de maîtrise numérique et la faiblesse des infrastructures rendent la région vulnérable. • Au Cameroun, les cyberincidents ont presque doublé en 2024. • Les fraudes aux cryptomonnaies et les escroqueries par manipulation psychosociale sont en hausse. • Les institutions financières doivent faire face à une augmentation des FOVI et des attaques sur leurs réseaux, tandis que la plupart des incidents sont clos sans suite du fait du manque de moyens en matière de cybersécurité.	Le numérique se développe plus rapidement que la préparation à la cybersécurité. • En 2024, l'Éthiopie était en tête du classement mondial en nombre de logiciels malveillants détectés, mettant en péril ses infrastructures critiques. • Les fraudes par échange de carte SIM augmentent en Ouganda et en Tanzanie. • La sextorsion et le harcèlement en ligne, qui visent particulièrement les femmes et les jeunes, sont de plus en plus répandus.	Le nombre de cyberattaques est grimpé en flèche en 2024, sous l'effet des tensions géopolitiques et de l'expansion du numérique. • L'Égypte et le Maroc ont été parmi les pays africains les plus visés, l'Égypte totalisant 13 % des attaques. • Les escroqueries par manipulation psychosociale et par hameçonnage, souvent via WhatsApp et avec de faux placements, sont monnaie courante.	La région africaine la plus développée en matière de cybersécurité n'est pas à l'abri des menaces. • Les hypertrucages et l'hameçonnage téléphonique basés sur l'IA ont connu une forte augmentation en 2024. • L'Afrique du Sud reste une cible privilégiée, en particulier ses institutions publiques et financières. • Le cryptominage pirate et l'hameçonnage par SMS se répandent en tirant parti de l'essor des entreprises de technologie financière.	La croissance rapide du numérique, en particulier des services bancaires mobiles et des réseaux sociaux, ont fait de l'Afrique de l'Ouest une plaque tournante de la cybercriminalité. • Les FOVI et les rançongiciels dominent la scène, avec des groupes basés au Nigéria tels que Black Axe et Opera1er à la tête d'escroqueries d'envergure mondiale. • Le Ghana a recensé près de 5 000 attaques DDoS début 2024, le secteur des télécommunications étant particulièrement visé. • Les fraudes liées aux portefeuilles mobiles et les escroqueries aux sentiments se multiplient, souvent liées à de faux placements dans les cryptomonnaies. • L'hameçonnage et les hypertrucages améliorés par l'IA représentent des menaces de plus en plus importantes.

Tableau 1 : tendances des cybermenaces et perspectives dans les sous-régions africaines

61 https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024

4. LES DÉFIS DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ EN AFRIQUE

4.1 Des cadres juridiques et politiques inégaux

La cybercriminalité continue de prendre le pas sur les systèmes juridiques qui sont conçus pour l'enrayer. Alors que 65 % des pays déclarent n'avoir apporté aucune modification à leur législation en matière de cybercriminalité au cours de l'année écoulée et plus de 75 % des pays estiment que leur cadre juridique et les capacités de leurs services judiciaires doivent être améliorés, il est clair que leurs systèmes juridiques présentent des lacunes importantes à combler[62].

Dans cette optique, plusieurs instruments internationaux et régionaux offrent des cadres permettant de renforcer la législation en matière de cybercriminalité :

- **Convention de Budapest sur la cybercriminalité[63] :** Fournit des lignes directrices complètes, dont l'article 19 qui décrit les compétences en matière d'accès aux données et de saisie. Seuls six pays africains l'ont ratifiée à ce jour.
- **Convention des Nations Unies contre la cybercriminalité[64] :** Cherchant à renforcer la coopération internationale dans la lutte contre la cybercriminalité, elle bénéficie d'un soutien croissant à travers l'Afrique.
- **Convention de Malabo de l'Union africaine[65] :** Mettant l'accent sur la cybersécurité et la protection des données personnelles, elle n'a été ratifiée que par 15 États membres de l'Union africaine à ce jour.

Ces lacunes soulignent la nécessité de plus en plus pressante d'une harmonisation avec les cadres juridiques internationaux, une question qui sera abordée plus en détail au chapitre 6.

4.2 Des contraintes en termes de capacités et de compétences

Des lois sévères ne constituent qu'une partie de la solution : la plupart des pays peinent également à les faire respecter. Les résultats de l'enquête montrent que **90 % des pays ayant répondu au sondage** estiment que leurs capacités en matière d'application de la loi ou de poursuites judiciaires doivent être « quelque peu » ou « considérablement » améliorées.

Les déficiences les plus courantes sont énoncées ci-après.

- **Besoins en formation :** 95 % des pays ont déclaré que la formation était insuffisante, incohérente ou dépendante des donateurs.
- **Ressources limitées :** 95 % des pays
- **Manque d'accès aux outils spécialisés :** 95 % des pays
- **Compétences techniques insuffisantes :** 74 % des pays
- **Infrastructures insuffisantes :** 72 % des pays
- **Obstacles opérationnels :** 58 % des pays sont confrontés à des obstacles bureaucratiques, juridiques ou institutionnels qui entravent l'efficacité des enquêtes.

Alors que le nombre d'incidents ne cesse d'augmenter, la plupart des pays ne disposent toujours pas des infrastructures essentielles pour lutter contre la cybercriminalité :

- **30 %** possèdent un système de signalement des incidents.
- **28 %** utilisent un système de gestion des dossiers.
- **19 %** disposent d'une base de données de renseignements sur les cybermenaces.
- **29 %** tiennent un référentiel d'éléments de preuve numériques.

De plus, peu d'institutions nationales disposent des effectifs ou des équipements nécessaires pour réagir avec la rapidité nécessaire. Les technologies malveillantes basées sur le cloud, les plateformes de messagerie cryptée et les enquêtes menées à l'échelle internationale dépassent souvent les capacités techniques et procédurales des équipes nationales.

62 Sondage d'évaluation des cybermenaces réalisé par INTERPOL

63 https://www.coe.int/fr/web/cybercrime/the-budapest-convention

64 https://www.unodc.org/unodc/fr/cybercrime/convention/text/convention-full-text.html

65 Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

4.3 De nouvelles menaces et des tactiques en constante évolution

En Afrique, la cybercriminalité repose de plus en plus sur de nouveaux outils et de nouvelles tactiques, qui ont souvent recours à l'intelligence artificielle, aux médias synthétiques et à la désinformation. Dans bon nombre de pays, les services nationaux n'ont pas la capacité de détecter ces menaces changeantes, d'enquêter à leur sujet ni de les contenir.

- **Hypertrucages (« deepfakes ») générés par l'IA et extorsion**

  Dans plusieurs pays, des escrocs se sont servi de vidéos hypertruquées ou du clonage vocal pour extorquer leurs victimes. Ces outils basés sur l'IA leur permettent en effet, sans même avoir besoin de connaissances techniques particulières, de réaliser des imitations très réalistes, de manipuler les émotions des personnes prises pour cible et de les soumettre à un chantage.
- **Campagnes de désinformation**

  Plusieurs services ont fait état d'affaires où des informations inventées de toutes pièces, des images modifiées et de faux comptes sur les réseaux sociaux ont été utilisés pour semer la panique, inciter à l'agitation publique ou nuire à la réputation de certaines personnes. Ces attaques visent généralement à saper la confiance des citoyens, en utilisant les canaux d'information publics comme arme.
- **L'essor des systèmes d'attaque clés en main**

  Les services d'hébergement complaisant sont de plus en plus utilisés comme plaques tournantes de la CaaS. Leurs offres permettent aux malfaiteurs, même novices, d'accéder à des kits d'hameçonnage, à des logiciels malveillants et à une automatisation évolutive hébergée sur une infrastructure conçue pour échapper aux mesures de désactivation.

En dépit de ces menaces en pleine évolution, 86 % des services ayant répondu au sondage n'ont pas encore intégré l'IA dans leurs opérations de maintien de l'ordre[66]. Alors que les pirates savent exploiter l'IA pour accroître la portée et l'efficacité de leurs supercheries, ce déficit de compétences chez les services de police risque de laisser de nombreux pays à la traîne.

4.4 Une coopération transfrontalière et un partage de renseignements limités

Alors que la cybercriminalité transgresse souvent les frontières, la plupart des pays africains rencontrent des difficultés à collaborer au niveau international. D'après les résultats de notre sondage, 86 % des services admettent que leur capacité de coopération transfrontalière devait être améliorée, et 44 % d'entre eux estiment même qu'elle devait l'être considérablement.

Un certain nombre de contraintes importantes ont été signalées à cet égard, telles que décrites ci-après.

- **Lenteur des procédures bureaucratiques :** Les procédures telles que les demandes d'entraide judiciaire et d'extradition sont souvent trop lentes pour pouvoir lutter efficacement contre la cybercriminalité, qui exige une rapidité de réaction. Ce constat souligne la nécessité de mettre en place des cadres de coopération plus souples et simplifiés.
- **Incohérences entre les pays sur le plan juridique et procédural :** Les différences existant d'un pays à l'autre entre les lois, les normes en matière d'éléments de preuve numériques et les réglementations relatives à la confidentialité des données sont autant de sources de friction qui entravent la collaboration. Ces aspects juridiques sont traités plus en détail au point 4.1.
- **Difficultés à construire des réseaux opérationnels et à instaurer la confiance :** Certains pays ont des difficultés à localiser ou à contacter leurs homologues étrangers, et les contacts établis ou les cadres de coordination en temps réel sont souvent limités, ce qui aboutit parfois à des occasions manquées d'action conjointe.
- **Accès limité aux plateformes et aux données hébergées à l'étranger :** Les services font état de difficultés à obtenir des informations auprès des plateformes ou des fournisseurs de services dont le siège social se trouve à l'étranger, en particulier dans les affaires impliquant des ressortissants étrangers ou des infrastructures situées dans d'autres pays.

Malgré ces obstacles, les opérations récentes coordonnées sous l'égide du projet AFJOC d'INTERPOL montrent que les interventions régionales de lutte contre la cybercriminalité peuvent s'avérer rapides et efficaces dès lors que des canaux fiables et des protocoles communs sont en place.

66 Sondage d'évaluation des cybermenaces réalisé par INTERPOL

4.5 Des obstacles aux partenariats public-privé et à la responsabilité des plateformes

Les enquêtes sur la cybercriminalité font de plus en plus appel à la coopération de partenaires du secteur privé, en particulier les plateformes technologiques, les fournisseurs de services de télécommunications et les institutions financières. Or, en Afrique, la plupart des services chargés de l'application de la loi se heurtent à des obstacles majeurs pour établir des relations avec ces partenaires.

- **Des mécanismes de coopération peu définis**

  Les services ont souvent des difficultés à accéder aux données d'entreprises telles que Meta, TikTok et Snapchat. À cet égard, ils invoquent l'absence de contacts directs, la lenteur des échanges et le manque de clarté des procédures à suivre. En l'absence d'accords officiels ou d'interlocuteurs désignés, leurs demandes sont souvent traitées tardivement, voire ignorées.

- **Un manque de préparation des institutions**

  Seuls quelques pays ont conclu un protocole d'accord ou des accords de partage de données avec des entreprises du secteur privé. Par ailleurs, de nombreux services n'ont pas les capacités techniques ou juridiques nécessaires pour formuler des demandes légalement recevables.

- **Une mobilisation insuffisante des secteurs des télécommunications et des technologies financières**

  À l'aune du rôle central qu'ils jouent dans les fraudes et les escroqueries, telles que la fraude par échange de carte SIM et l'utilisation frauduleuse des services de paiement par téléphone mobile, les fournisseurs de services de télécommunications et de services financiers restent des partenaires trop peu sollicités dans les stratégies nationales de lutte contre la cybercriminalité.

→ D'après le sondage, 89 % des pays africains estiment que leur coopération avec le secteur privé devait être « quelque peu » ou « considérablement » améliorée[67].

À mesure que le secteur privé prend le contrôle des infrastructures numériques, la capacité des services chargés de l'application de la loi à intervenir dépendra de plus en plus de l'accès qui leur sera accordé, de la confiance de ces partenaires et d'une coopération méthodique, autant d'éléments qui ne peuvent être laissés au hasard.

67 Sondage d'évaluation des cybermenaces réalisé par INTERPOL

5. AVANCÉES DANS LE DOMAINE DE LA CYBERSÉCURITÉ EN AFRIQUE

L'Afrique a réalisé des progrès notables en matière de cybersécurité, grâce à des réformes juridiques, des avancées dans le domaine de la criminalistique, des initiatives de sensibilisation du public, une amélioration de la coopération régionale et l'adoption grandissante des nouvelles technologies. Ces avancées témoignent d'une mobilisation croissante en faveur de la lutte contre la cybercriminalité et d'un renforcement de la sécurité numérique sur l'ensemble du continent.

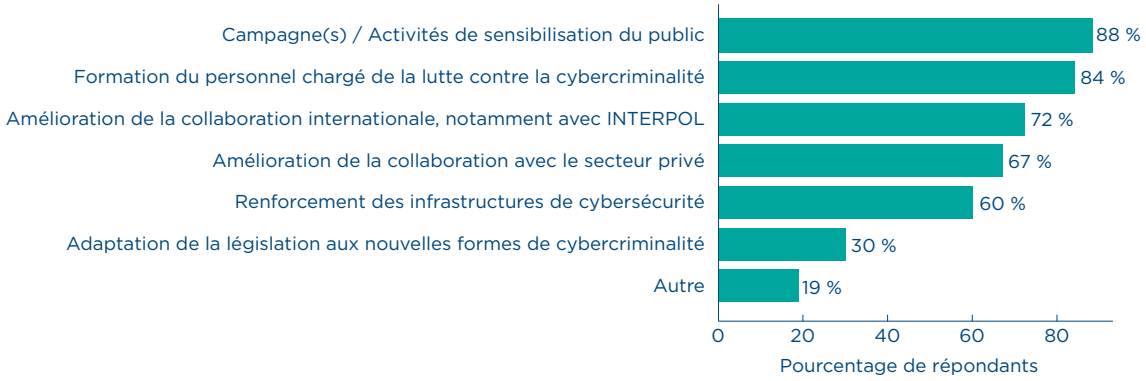


Figure 8. Mesures préventives contre la cybercriminalité mises en œuvre par les services chargés de l'application de la loi dans les pays africains en 2024

5.1 Renforcement des cadres nationaux de lutte contre la cybercriminalité

En 2024, plusieurs pays africains ont renforcé leurs cadres juridiques pour lutter contre la cybercriminalité, ce qui traduit un engagement croissant en faveur de la sécurité numérique.

- La **Tunisie** est devenue la 70ème Partie à la Convention de Budapest sur la cybercriminalité en mars 2024, mettant ainsi son cadre juridique en consonance avec les normes internationales afin de faciliter la coopération transfrontalière dans la lutte contre la cybercriminalité.
- Le **Nigéria** a promulgué en 2024 une loi sur les cyberinfractions (interdiction, prévention, etc.) (modification), qui met à jour sa législation datant de 2015. Les principaux changements apportés par cette loi comprennent la création de cellules de crise sectorielles appelées à répondre aux urgences informatiques (CERT), la clarification des dispositions relatives au cyberharcèlement et l'établissement d'une taxe sur la cybersécurité destinée à financer des initiatives à l'échelle nationale[68].
- La **Gambie** a présenté son premier projet de loi dédié à la lutte contre la cybercriminalité (2023) au Parlement, posant ainsi la première pierre de sa stratégie officielle dans ce domaine[69].
- La **Guinée-Bissau** a mis au point sa stratégie nationale de cybersécurité en 2024[70] tout en réalisant des progrès significatifs dans le cadre de ses efforts plus généraux de transformation numérique. En janvier 2025, le gouvernement a officiellement lancé la Stratégie nationale pour la transformation numérique, visant à renforcer le développement économique, la gestion des données, la gouvernance et les services publics[71].
- En juillet 2024, le **Burkina Faso** a adopté la loi 014-2024/ALT, qui vient renforcer la protection des systèmes d'information et encadrer les réponses à apporter aux cybermenaces, notamment les rançongiciels et les escroqueries en ligne[72].

Tous ces efforts législatifs illustrent la tendance régionale à harmoniser les lois sur la cybersécurité avec les normes internationales, en faisant notamment référence à la Convention de Budapest et à la Convention des Nations Unies contre la cybercriminalité.

68 https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/
69 https://mocde.gov.gm/ministry-of-communications-and-digital-economy-of-the-gambia-embarked-on-a-two-day-retreat-to-discuss-the-cybercrime-bill-2023/
70 Sondage d'évaluation des cybermenaces réalisé par INTERPOL
71 https://unu.edu/egov/news/digital-transformation-project-guinea-bissau-egov-undp
72 https://www.mdenp.gov.bf/fileadmin/user_upload/storages/documents/administratifs/loi_014_systeme_d_information.pdf

5.2 Amélioration des capacités institutionnelles et techniques

Au cours des 18 derniers mois, les pays africains ont nettement amélioré leurs capacités de lutte contre la cybercriminalité. Les investissements réalisés dans des unités spécialisées, dans les infrastructures de criminalistique numérique et dans le renforcement des capacités ont contribué de manière décisive à accroître l'efficacité des enquêtes et de l'application de la loi.

- D'après les résultats du sondage[73], **67 %** des pays participants ont déclaré avoir organisé des activités de renforcement des capacités liées à la lutte contre la cybercriminalité en 2024, tandis que **44 %** ont affirmé avoir créé de nouvelles unités de lutte contre la cybercriminalité ou avoir élargi celles qui étaient déjà en place.
- **Algérie :** Fin 2023, l'Algérie a inauguré le nouveau siège national de son Service central de lutte contre la cybercriminalité et étendu les opérations de ce dernier à l'ensemble de ses 58 provinces. Les services sont désormais répartis par fonction (surveillance, assistance technique et enquêtes), ce qui permet de mieux coordonner l'action policière. Ces réformes structurelles sont consolidées par des activités de formation continue[69, 74].
- **Seychelles :** Après la création de son service de lutte contre la cybercriminalité en 2023[77], la Police des Seychelles a reçu au cours des 18 derniers mois une série d'outils numériques et de supports de formation de la part du Gouvernement britannique[75] ainsi qu'un laboratoire de criminalistique numérique offert par le Gouvernement chinois[76]. Ces nouveaux outils ont pour vocation d'améliorer les enquêtes cybernétiques et la qualité du traitement des éléments de preuve numériques.
- **Bénin :** Le gouvernement a créé le Centre national d'investigations numériques (CNIN) afin de centraliser les enquêtes sur la cybercriminalité et les activités de criminalistique numérique[78]. En août 2024, le CNIN a annoncé le démantèlement d'un important réseau cybercriminel à Comè, démontrant ainsi son efficacité opérationnelle[79].
- **Togo :** Dans le cadre de sa stratégie nationale de cybersécurité pour 2024-2028, le Togo renforce son dispositif de lutte contre la cybercriminalité en mettant en place une entité unique à cette fin[80], a ouvert un nouveau laboratoire de criminalistique numérique[69] et continue d'investir dans la formation technique du personnel chargé des enquêtes.
- **Congo :** Fin 2024, le gouvernement a organisé une formation spécialisée à l'intention des services chargés de l'application de la loi et des autorités judiciaires, portant sur le recueil des éléments de preuve numériques et sur les techniques d'enquête en matière de cybercriminalité[81].

Ces progrès sont le miroir d'une transition plus large à l'échelle du continent, où les mesures jusqu'alors fragmentées ou discontinues de lutte contre la cybercriminalité font progressivement place à une dynamique plus structurée, dotée de davantage de moyens et de plus en plus axée sur la technologie. Pour consolider et amplifier ces acquis, il sera essentiel de continuer à investir dans les infrastructures, la formation du personnel et la coordination interservices.

73 Sondage d'évaluation des cybermenaces réalisé par INTERPOL
74 https://www.horizons.dz/?p=74105
75 http://www.seychellesnewsagency.com/articles/19082/British+government+donates+digital+tech+to+Seychelles+Police+Force+for+better+training+and+results
76 http://www.seychellesnewsagency.com/articles/19616/China+gifts+Seychelles+Police+Force+digital+forensic+lab+to+help+deal+with+cybercrime
77 https://www.nation.sc/articles/16639/cybercrime-unit-in-the-offing--by-vidya-gappy
78 https://cybersecuritymag.africa/benin-renforce-lutte-contre-cybercriminalite-avec-creation-du-cnin
79 https://cybersecuritymag.africa/index.php/le-cnin-demantele-un-vaste-reseau-de-cybercriminels-come-au-benin
80 https://www.togofirst.com/fr/justice/2705-14106-au-togo-vers-la-creation-d-une-entite-unique-de-lutte-contre-la-cybercriminalite
81 https://www.wearetech.africa/en/fils-uk/news/tech/congo-hosts-cybersecurity-training-for-judicial-and-law-enforcement

5.3 Renforcement de la cyberrésilience grâce à la sensibilisation du public

En 2024, 88 % des pays africains ont déclaré mener des campagnes de sensibilisation du public ou des projets pédagogiques visant à prévenir la cybercriminalité. Il s'agit donc de l'activité préventive la plus répandue sur le continent.

Généralement conçues à l'intention des groupes vulnérables tels que les étudiants, les jeunes, les propriétaires de petites entreprises et les personnes âgées, ces initiatives reposent sur plusieurs méthodes de communication, passant notamment par la télévision nationale, la radio, les réseaux sociaux, les alertes par SMS et les programmes scolaires.

1. Campagnes auprès des jeunes et dans les écoles

La sensibilisation des jeunes publics est une priorité stratégique pour de nombreux pays, afin de promouvoir la sécurité en ligne, la lutte contre le cyberharcèlement et la maîtrise numérique.

- **Eswatini :** Le ministère des TIC, en collaboration avec la Commission des communications d'Eswatini et l'UNESCO, a organisé des séances de sensibilisation à la cybersécurité dans les écoles[82, 83, 84].
- **Afrique du Sud :** L'Institut des professionnels des technologies de l'information d'Afrique du Sud (IITPSA), par l'intermédiaire de son groupe d'intérêt spécial pour la cybersécurité (SIGCyber), a organisé le premier procès simulé sur la cybersécurité à Gqeberha. Face à un cas fictif de cyberharcèlement, des lycéens devaient présenter leurs arguments devant un jury, l'objectif étant de les aider à mieux comprendre les torts que peut causer le monde numérique et les solutions possibles à mettre en place au niveau des établissements scolaires[85].
- **Maroc :** La police a mené des projets de sensibilisation dans les écoles en partenariat avec le ministère de l'Éducation. Par ailleurs, en mai 2024, plus de 2,1 millions de personnes ont participé aux journées portes ouvertes organisées par la Direction générale de la Sûreté nationale à Agadir, consistant en des expositions sur la cybercriminalité, la participation d'élèves de 845 écoles et le lancement de la plateforme de signalement de contenus cybercriminels E-Blagh[86, 87].
- Dans le cadre de la stratégie pour un internet mieux adapté aux enfants[89], des organisations de la société civile telles que Child Online Africa[88] ont organisé des initiatives comme la Journée pour un Internet plus sûr en Afrique, le Concours sur la sécurité et le bien-être en ligne et la Semaine de la maîtrise numérique, qui s'adressent aux établissements scolaires, aux parents et aux institutions religieuses.

2. Mobilisation des médias et des réseaux sociaux

Afin d'atteindre un public aussi large que possible, les pays s'appuient de plus en plus sur les réseaux sociaux et les médias pour diffuser des messages de prévention contre la cybercriminalité.

- **Ghana :** En octobre 2024, l'Autorité chargée de la cybersécurité (CSA) a lancé le Mois national de sensibilisation à la cybersécurité sur le thème « Lutter contre la mésinformation/désinformation dans une démocratie numérique résiliente - Notre responsabilité à tous ». La campagne comprenait une série d'actions médiatiques à l'échelle nationale, des forums régionaux et des initiatives de sensibilisation du public cherchant à renforcer la résilience numérique avant les élections nationales[90].
- **Rwanda :** L'Autorité nationale de la cybersécurité (NCSA) a mené sa campagne annuelle « Tekana Online » tout au long du mois d'octobre 2024. S'appuyant sur la télévision, la radio et les réseaux sociaux, cette initiative entend sensibiliser les citoyens et leurs familles, ainsi que les entreprises et autres organisations, aux meilleures pratiques à suivre en matière de lutte contre les cybermenaces telles que les escroqueries en ligne, les rançongiciels et l'hameçonnage[91].
- **INTERPOL :** En décembre 2024, INTERPOL a mené la campagne #ThinkTwice sur les réseaux sociaux. Cette campagne visait à sensibiliser le public aux cybermenaces, notamment aux rançongiciels, à l'hameçonnage et aux escroqueries portées par l'IA générative, en encourageant les internautes à prendre des décisions avisées lorsqu'ils naviguent sur la toile[92].

82 https://independentnews.co.sz/10470/local-news/cybersecurity-awareness-initiative-hits-schools/
83 https://www.facebook.com/story.php?id=100069400350741&story_fbid=850193827303955&
84 https://www.swazilandnews.co.za/fundza.php?nguyiphi=7578&
85 https://www.itweb.co.za/article/iitpsa-sigcyber-raises-awareness-on-cyber-bullying-at-inaugural-moot-court-event/6GxRKqYQrnmqb3Wj
86 https://www.mapnews.ma/fr/actualites/social/jpo-de-la-dgsn-un-nombre-record-de-2120000-visiteurs
87 https://fr.hespress.com/371518-la-dgsn-lance-la-nouvelle-plateforme-e-blagh-dediee-a-la-lutte-contre-la-cybercriminalite.html
88 https://www.childonlineafrica.org/
89 https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/africa-safer-internet-day
90 ncsam.csa.gov.gh
91 https://cyber.gov.rw/updates/article/ncsa-launches-cybersecurity-and-data-protection-awareness-campaign/
92 https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/Une-campagne-INTERPOL-met-en-garde-contre-la-cybercriminalite-et-la-criminalite-financiere

3. Sensibilisation communautaire et culturelle
Les campagnes ciblées utilisant un langage familier et s'appuyant sur la culture locale sont particulièrement efficaces dans les communautés rurales et isolées.

- **Tchad :** À N'Djamena, les pouvoirs publics ont mis en place des projets de sensibilisation à la cybercriminalité faisant appel à des artistes locaux et à des stations de radio privées, un choix stratégique dans un pays où l'alphabétisation n'est pas donnée à tous et où de nombreuses communautés privilégient la communication orale. Conçues pour sensibiliser les habitants aux escroqueries en ligne, ces campagnes ont été réalisées dans les langues locales, avec des messages adaptés sur le plan culturel, ce qui a permis de diffuser l'information auprès de groupes de population avec lesquels il est difficile de communiquer via des supports écrits ou des contenus numériques[93].
- **République démocratique du Congo :** Tous les mois, la Police organise des réunions publiques afin de restituer à leurs propriétaires les téléphones volés qu'elle a récupérés. Menée en partenariat avec l'autorité nationale de réglementation des télécommunications et le Parquet, cette initiative fait l'objet d'une large publicité et entend dissuader les consommateurs d'acheter des téléphones d'occasion. Ces appareils sont en effet souvent associés à des cyberinfractions, telles que l'usurpation d'identité, l'extorsion et la diffamation. Cette campagne a permis de sensibiliser grandement le public tout en contribuant à réduire ce type d'infractions[89].

4. Diffusion par des canaux institutionnels et intersectoriels
Quelques campagnes de sensibilisation parmi les plus influentes d'Afrique sont menées par des structures coordonnées, auxquelles prennent part plusieurs ministères, services chargés de l'application de la loi et groupes de la société civile. Ces partenariats institutionnels améliorent la portée et la cohérence des messages, tout comme leur crédibilité.

- **Algérie :** Les services algériens spécialisés dans la lutte contre la cybercriminalité ont travaillé en étroite collaboration avec le ministère de l'Éducation, le ministère de la Poste et des Télécommunications et des organisations de la société civile afin de mener des campagnes de sensibilisation du public. Celles-ci ciblaient divers groupes de population et ont été diffusées avec régularité par différents moyens, notamment à la radio, à la télévision, sur les réseaux sociaux, dans des forums publics et à travers des annonces. Les autorités ont pu constater l'efficacité de ces campagnes par les réactions dans les réseaux sociaux, l'augmentation du nombre de signalements de cyberinfractions et l'adoption de comportements préventifs par la population en général.

5.4 Renforcement des opérations des services chargés de l'application de la loi

En 2024, le renforcement des capacités opérationnelles des pays africains et de leur collaboration à l'échelle internationale a été mis en exergue lors de deux opérations internationales de lutte contre la cybercriminalité de grande envergure coordonnées par INTERPOL.

- L'**opération Serengeti** (septembre - octobre 2024) a été l'une des interventions les plus importantes menées à ce jour sur le continent dans le domaine de la lutte contre la cybercriminalité. Coordonnée par INTERPOL et AFRIPOL, et concernant 19 pays africains, cette opération a abouti à l'arrestation de plus d'un millier de personnes, au démantèlement de 134 000 infrastructures malveillantes en ligne et à l'identification de plus de 35 000 victimes. Les autorités ont ciblé les utilisateurs de rançongiciels, les escrocs aux FOVI, les racketteurs numériques et les réseaux d'escroquerie aux placements en ligne. Au total, les pertes financières à l'échelle mondiale imputables aux activités frauduleuses auxquelles l'opération a mis un terme ont été estimées à 193 millions d'USD. Des partenaires du secteur privé, notamment des fournisseurs d'accès à Internet, ont soutenu l'opération en aidant à démanteler des infrastructures et à sécuriser des plateformes numériques[94].
- L'**opération Red Card** (octobre 2024 - mars 2025), menée sous l'égide du projet AFJOC, a réuni les services chargés de la lutte contre la cybercriminalité de Côte d'Ivoire, du Bénin, du Togo, du Rwanda, d'Afrique du Sud, de Zambie et du Nigéria. Cette opération a permis de démanteler un réseau d'escroquerie aux prêts en ligne en analysant des domaines, des fichiers APK et des profils sur les réseaux sociaux. Les renseignements fournis par le secteur privé ont contribué à étayer les rapports élaborés sur les activités cybernétiques, qui ont joué un rôle déterminant dans le repérage des infrastructures criminelles et l'identification des cybermalfaiteurs[95].

Ces deux opérations témoignent d'une capacité croissante des pays africains à prendre part à des enquêtes transfrontalières complexes sur la cybercriminalité, grâce à une meilleure coordination, à des mécanismes de partage de renseignements et à une collaboration entre le secteur public et le secteur privé.

93 Sondage d'évaluation des cybermenaces réalisé par INTERPOL
94 https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects
95 https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats

6. RECOMMANDATIONS ET CONCLUSION

En réponse aux menaces, aux défis systémiques et aux lacunes en matière de capacités mis en évidence dans le cadre de cette évaluation, INTERPOL propose les recommandations stratégiques suivantes, formulées à l'intention des services chargés de l'application de la loi, des responsable des politiques, des organismes régionaux et des partenaires internationaux. Ces recommandations s'appuient sur les commentaires fournis par les pays membres, les enseignements tirés des opérations et les tendances observées. Leur objectif est de susciter une amélioration durable, pratique et coordonnée des capacités de lutte contre la cybercriminalité en Afrique.

Elles sont classées en six volets thématiques :

- Le renforcement des capacités au niveau national.
- La consolidation des cadres juridiques et politiques.
- L'amélioration de la coopération régionale et internationale.
- Le développement de la prévention et de la sensibilisation du public.
- L'approfondissement des partenariats public-privé.
- La mise à profit des nouvelles technologies pour la prévention de la cybercriminalité.

6.1 Le renforcement des capacités au niveau national

Les services chargés de l'application de la loi des pays africains doivent être soutenus pour acquérir les capacités opérationnelles, techniques et institutionnelles dont ils ont besoin pour détecter la cybercriminalité, enquêter à son sujet et y faire obstacle le plus efficacement possible. Si nombre de pays ont fait des progrès, des disparités persistent à travers le continent. Les mesures recommandées en priorité sont les suivantes :

- mettre en place et développer des unités spécialisés dans la lutte contre la cybercriminalité, dotées d'effectifs, d'un mandat et de moyens techniques suffisants au niveau national ;
- investir dans des formations spécifiques à la cybercriminalité destinées aux enquêteurs, analystes, procureurs et juges, notamment dans des domaines tels que la criminalistique numérique, l'analyse des logiciels malveillants, les renseignements provenant de sources publiques et le suivi des avoirs ;
- assurer un accès durable à des outils d'enquête modernes, notamment à des logiciels de criminalistique numérique sous licence et à un système de stockage sécurisé des éléments de preuve numériques ;
- créer et mettre en service des cellules d'intervention en cas d'atteinte à la cybersécurité (CIRT) dotées de protocoles clairs concernant la coordination interservices ;
- fidéliser les agents spécialisés dans la lutte contre la cybercriminalité grâce à des opportunités de carrière bien définies et à des mesures incitatives, afin de réduire la fuite des cerveaux et de garantir l'efficacité des services à long terme.

Un investissement soutenu pour améliorer les capacités au niveau national est la clé de voûte d'une infrastructure efficace et autonome de lutte contre la cybercriminalité.

6.2 La consolidation des cadres juridiques et politiques

La lutte contre la cybercriminalité dépend de l'existence de cadres juridiques solides, mis à jour et exécutoires. Cependant, de nombreux pays africains se heurtent encore à des écueils législatifs qui entravent leur capacité à poursuivre les cybermalfaiteurs, à accéder aux éléments de preuve d'autres pays ou à coopérer au niveau international.

Pour surmonter ces difficultés, INTERPOL recommande les mesures suivantes :

- accélérer l'adoption et la mise en œuvre de lois nationales détaillées sur la cybercriminalité, en consonance avec les normes internationales et traitant à la fois les infractions commises contre des systèmes informatiques et celles facilitées par l'utilisation d'Internet ;
- garantir la reconnaissance juridique et l'admissibilité des éléments de preuve numériques, y compris ceux provenant d'un autre pays ;
- harmoniser les définitions juridiques et les procédures d'un pays à l'autre, afin de réduire la fragmentation juridique du continent et de permettre une coopération plus efficace au niveau régional ;
- ratifier et mettre en œuvre des conventions internationales et régionales, telles que la Convention de Budapest sur la cybercriminalité, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) et la Convention des Nations Unies contre la cybercriminalité ;
- définir des procédures juridiques claires permettant un accès rapide aux données détenues par des plateformes basées à l'étranger, notamment par l'intermédiaire de traités d'entraide judiciaire ou de mécanismes de divulgation d'informations en cas d'urgence.

Il est indispensable d'entreprendre des réformes juridiques pour renforcer la confiance dans les capacités des services chargés de l'application de la loi et faire en sorte que les auteurs de cyberinfractions aient à répondre de leurs actes. Ces mesures doivent s'accompagner d'investissements dans la formation des magistrats et la spécialisation des parquets.

6.3 L'amélioration de la coopération régionale et internationale

En raison de la nature transnationale de la cybercriminalité, aucun pays n'est en mesure de s'attaquer seul aux menaces qu'elle représente. La coopération régionale et internationale est indispensable pour pouvoir mener des enquêtes transfrontalières, démanteler les infrastructures des cybermalfaiteurs et partager des renseignements en temps réel.

Pour renforcer les capacités de riposte collective, INTERPOL recommande les mesures suivantes :

- ratifier et mettre en œuvre les traités internationaux relatifs à la cybercriminalité, tels que la Convention des Nations Unies contre la cybercriminalité et la Convention de Budapest sur la cybercriminalité, afin de faciliter les enquêtes transfrontalières et l'extradition des cybermalfaiteurs ;
- renforcer les mécanismes d'échange de renseignements entre les pays africains en élargissant la participation à l'AFJOC et à d'autres programmes régionaux et internationaux de lutte contre la cybercriminalité.
- institutionnaliser les mécanismes qui permettent les enquêtes transfrontalières, en prévoyant notamment des procédures officielles de partage des éléments de preuve, de signalement et d'enquêtes parallèles ;
- utiliser des plateformes de communication sécurisées, comme le système I-24/7 d'INTERPOL, pour assurer une coordination rapide des services chargés de l'application de la loi dans différents pays ;
- soutenir les opérations conjointes et les équipes plurinationales axées sur le démantèlement des réseaux cybercriminels opérant dans la région.

INTERPOL et AFRIPOL sont déterminés à faciliter une coopération bien structurée à travers le continent africain et avec leurs partenaires dans le monde entier. Une collaboration soutenue sera essentielle pour combler les lacunes en matière d'application de la loi et combattre les groupes cybercriminels organisés qui font fi des frontières nationales.

6.4 Le développement de la prévention et de la sensibilisation du public

Si les moyens techniques et les outils juridiques sont essentiels pour lutter contre la cybercriminalité, la prévention reste la première ligne de défense. Peu coûteuse au regard de son efficacité, elle peut en outre être déployée à grande échelle. En Afrique, de nombreuses formes de cybercriminalité, telles que l'hameçonnage, les escroqueries en ligne et l'escroquerie aux sentiments, ont recours à la manipulation psychosociale et mettent à profit la faible maîtrise du numérique au sein de la population.

Afin de renforcer la prévention, INTERPOL recommande les mesures suivantes :

- lancer des campagnes de sensibilisation ciblées, en particulier à l'intention des groupes à haut risque tels que les jeunes, les femmes, les petites et moyennes entreprises (PME) et les internautes débutants ;
- intégrer l'éducation à la cybersécurité dans les programmes scolaires, la formation professionnelle et les programmes d'apprentissage pour adultes ;
- promouvoir une série de bonnes pratiques élémentaires en matière de cybersécurité, telles que l'utilisation de mots de passe sûrs, l'authentification à facteurs multiples et le signalement des messages suspects ;
- encourager les victimes à signaler les incidents, en renforçant la confiance dans les services chargés de l'application de la loi et en garantissant la confidentialité, en particulier dans les affaires de sextorsion ou d'escroquerie en ligne ;
- mettre à contribution les organisations de la société civile locale, y compris les groupes de femmes et les réseaux de jeunes, pour diffuser des messages de prévention adaptés sur le plan culturel.

En donnant aux individus et aux communautés les moyens de détecter les cybermenaces et de les éviter, les pays seront en mesure de réduire le nombre de victimes potentielles et effectives des cybermalfaiteurs et pourront ainsi alléger la charge des enquêtes qui pèse sur les services chargés de l'application de la loi.

6.5 L'approfondissement des partenariats public-privé

Les enquêtes sur la cybercriminalité sont souvent tributaires des données, des infrastructures et des connaissances détenues par des entités du secteur privé, notamment les fournisseurs de services de télécommunications, les institutions financières, les plateformes de réseaux sociaux et les entreprises de cybersécurité. Or, les services chargés de l'application de la loi dans les pays africains se heurtent toujours à des obstacles pour accéder rapidement aux informations en possession de ces acteurs et bénéficier de leur soutien technique.

En vue d'instaurer un environnement plus collaboratif, INTERPOL recommande les mesures suivantes :

- formaliser les modalités de coopération entre les services chargés de l'application de la loi et les principaux acteurs du secteur privé, en établissant notamment des mécanismes officiels permettant un partage sécurisé et légal des données ;
- créer des instances de coordination de la lutte contre la cybercriminalité aux niveaux national et régional et rejoindre celles qui sont déjà en place (par exemple, le Groupe d'experts mondial d'INTERPOL sur la cybercriminalité), afin de réunir les organismes de réglementation, les enquêteurs, les procureurs et les acteurs du secteur privé en vue de faire converger les priorités et de partager des renseignements ;
- faciliter la consultation rapide des éléments de preuve numériques provenant de plateformes mondiales, grâce à des accords juridiques plus efficaces, au moyen de protocoles techniques définis et via des canaux de communication fiables ;
- tirer parti de l'expertise et des infrastructures du secteur privé dans des domaines tels que les renseignements sur les menaces, l'analyse des logiciels malveillants et la réponse aux incidents ;
- encourager la participation du secteur privé aux initiatives de renforcement des capacités, notamment par l'intermédiaire de formations, de boîtes à outils et de programmes de mentorat destinés au personnel du secteur public.

En favorisant un climat de confiance et de rapprochement opérationnel entre le secteur public et le secteur privé, les pays pourront disposer de moyens déterminants pour accélérer le démantèlement des réseaux cybercriminels.

6.6 La mise à profit des nouvelles technologies pour la prévention de la cybercriminalité

À mesure que les cybermenaces évoluent, les outils et les stratégies utilisés pour les combattre doivent faire de même. L'intelligence artificielle, l'apprentissage automatique, l'analyse de données et l'automatisation sont autant d'instruments qui offrent aux services chargés de l'application de la loi de nouvelles possibilités pour anticiper les forfaits des cybermalfaiteurs, les détecter et y faire obstacle à grande échelle. Cependant, le degré d'adoption de ces technologies varie encore considérablement d'un pays à l'autre en Afrique.

En vue de promouvoir une démarche plus proactive et fondée sur les données, INTERPOL recommande les mesures suivantes :

- étudier les possibilités offertes par l'IA et les outils d'apprentissage automatique pour détecter l'hameçonnage, déceler les anomalies et classer les éléments de preuve numériques ;
- renforcer les capacités d'analyse des données aux niveaux national et régional pour pouvoir suivre les tendances de la cybercriminalité et favoriser la surveillance des menaces en temps réel ;
- investir dans une infrastructure cloud sécurisée pour la gestion des dossiers, la criminalistique numérique et l'échange d'informations entre pays ;
- tester des outils d'automatisation pour le recueil d'éléments de preuve, la résolution des incidents et la surveillance des réseaux au sein des services chargés de l'application de la loi ;
- mettre en place des cadres éthiques et juridiques pour veiller à une utilisation responsable des nouvelles technologies dans les enquêtes sur la cybercriminalité, en s'inspirant des initiatives du Centre d'innovation d'INTERPOL en matière d'intelligence artificielle.

Les nouvelles technologies ouvrent la voie à une action plus rapide, plus intelligente et plus évolutive, à condition d'être employées avec prudence et assorties de garanties appropriées.

À PROPOS D'INTERPOL

INTERPOL est la plus grande organisation internationale de police au monde. Son rôle est d'assister les services chargés de l'application de la loi de nos 196 pays membres dans la lutte contre toute forme de criminalité transnationale. Il s'emploie à aider les polices du monde entier à relever les défis (de plus en plus nombreux) de la lutte contre la criminalité au XXIème siècle en leur apportant un appui technique et opérationnel grâce à une infrastructure de pointe. Les services de l'Organisation comprennent des formations ciblées, un soutien spécialisé aux enquêtes, des bases de données spécialisées et un système de communication policière sécurisé.

LA VISION D'INTERPOL : RELIER LES POLICES POUR UN MONDE PLUS SÛR

La vision d'INTERPOL est celle d'un monde dans lequel chaque professionnel des services chargés de l'application de la loi pourra, par la voie de l'Organisation, transmettre, échanger et consulter en toute sécurité des informations de police vitales, à tout moment et en tout lieu où il en aura besoin, afin d'assurer la sécurité des personnes sur toute la surface du globe. INTERPOL apporte et travaille à offrir continuellement des solutions innovantes et de pointe aux problèmes qui se posent à l'échelle mondiale en matière de police et de sécurité.

À PROPOS DU PROGRAMME INTERPOL DE LUTTE CONTRE LA CYBERCRIMINALITÉ

Dans un monde numérique dynamique où plus de la moitié de la population mondiale est susceptible d'être exposée à la cybercriminalité, le Programme mondial INTERPOL de lutte contre la cybercriminalité fournit un appui à la communauté internationale des services chargés de l'application de la loi. Nous sommes déterminés à préparer et piloter une riposte mondiale visant à prévenir et détecter la cybercriminalité, ainsi qu'à enquêter à son sujet et y faire obstacle, avec l'objectif ultime d'aider les pays membres à combattre plus efficacement la cybercriminalité transnationale.

La Stratégie mondiale INTERPOL de lutte contre la cybercriminalité a quatre objectifs principaux :

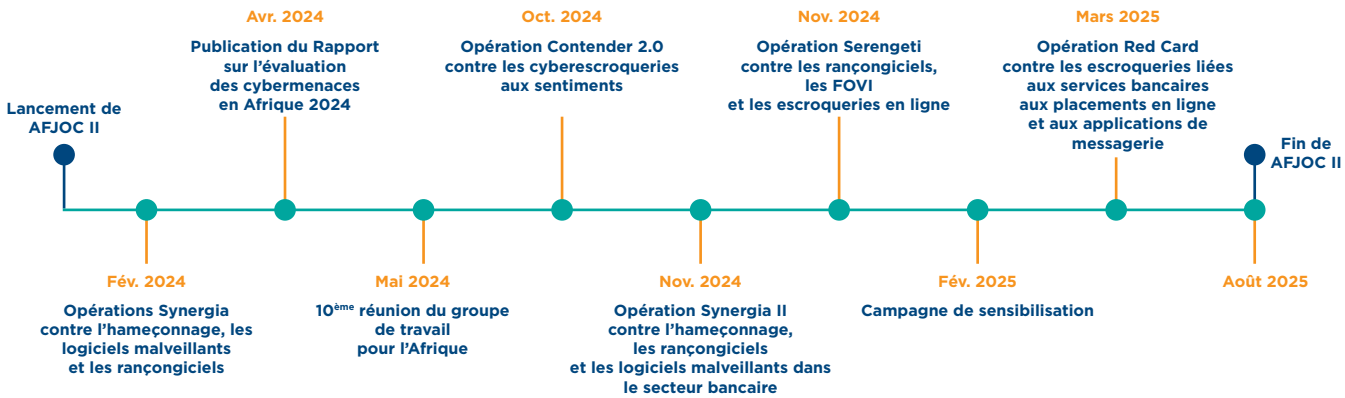
- Favoriser une démarche proactive et agile en matière de prévention et de répression de la cybercriminalité, en cernant en profondeur le paysage des cybermenaces grâce à l'échange d'informations et l'analyse de renseignements.
- Agir avec efficacité pour prévenir et détecter la cybercriminalité, qui cause des préjudices importants à l'échelle nationale, régionale et mondiale, ainsi qu'enquêter à son sujet et y faire obstacle, en jouant un rôle de direction, de coordination et d'appui auprès des pays membres dans le cadre d'activités opérationnelles transnationales.
- Appuyer l'élaboration des stratégies et le renforcement des capacités des pays membres en matière de lutte contre la cybercriminalité en nouant des partenariats ouverts, inclusifs et pluriels, et en instaurant la confiance dans l'écosystème mondial de la cybersécurité.
- Promouvoir le rôle et les capacités d'INTERPOL dans le processus visant à façonner la sécurité mondiale via la participation à des instances internationales dans le domaine de la cybercriminalité.

Notre Stratégie et ses objectifs sont mis en œuvre selon un modèle simple et constructif, reposant sur trois grands piliers :

- Réponse aux cybermenaces : Apporter une réponse rapide et coordonnée aux cybermenaces immédiates et émergentes.
- Opérations de lutte contre la cybercriminalité : Mettre en œuvre des stratégies opérationnelles régionales et mondiale pour lutter efficacement contre la cybercriminalité.
- Renforcement des capacités en matière de cybercriminalité : Renforcer les stratégies et les capacités via des plateformes et projets innovants.

Ces piliers s'appuient sur notre vaste réseau de partenaires publics et privés, qui encourage la collaboration et tire parti de l'expertise collective pour lutter contre la cybercriminalité.

Pour de plus amples informations, nous vous invitons à contacter la Direction de la Cybercriminalité d'INTERPOL à l'adresse suivante : EDPS-CD@interpol.int



À PROPOS DE L'OPÉRATION CONJOINTE DE LUTTE CONTRE LA CYBERCRIMINALITÉ EN AFRIQUE D'INTERPOL

Le projet AFJOC est une initiative menée par INTERPOL qui vise à renforcer les capacités des services nationaux chargés de l'application de la loi en Afrique en matière de prévention, de détection, d'enquête et de lutte contre la cybercriminalité. Pour y parvenir, il s'attelle à :

- recueillir et analyser les informations relatives aux activités cybercriminelles ;
- mener des actions coordonnées et fondées sur le renseignement ;
- promouvoir la coopération et les bonnes pratiques dans les pays africains.

La phase 1 de l'initiative, qui s'est déroulée de 2021 à 2023, a été financée par le Bureau britannique des Affaires étrangères, du Commonwealth et du Développement. La phase 2, qui bénéficie toujours du soutien du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement, s'appuie sur les réalisations de la première phase et vise à renforcer encore davantage les capacités des services nationaux chargés de l'application de la loi en Afrique.

Activités menées dans le cadre du projet

- Soutien en matière d'analyse et renseignement : des renseignements exacts et obtenus en temps utile sont la clé de toute riposte efficace contre la cybercriminalité. Nos signalements d'activités cybercriminelles constituent d'importantes ressources, qui répertorient les cybermenaces ciblant certains pays ou régions.
- Renforcement des capacités et moyens régionaux de lutte contre la cybercriminalité : des plateformes collaboratives telles que la Plateforme collaborative sur la cybercriminalité et la Plateforme de fusionnement sur la cybercriminalité facilitent la communication et l'échange sécurisés de données sur les opérations.
- Cadre opérationnel conjoint : il cible les cybermenaces via la collaboration entre les services chargés de l'application de la loi, le secteur privé et d'autres organisations internationales ou intergouvernementales.
- Appui opérationnel et coordination : nos opérations contribuent au démantèlement des réseaux cybercriminels.
- Campagnes de sensibilisation : promotion de bonnes pratiques informatiques auprès des particuliers et des entreprises en Afrique.
- Réunions du groupe de travail des chefs d'unité : elles rassemblent des représentants de presque tous les pays africains afin de traiter des défis régionaux liés à la cybercriminalité et de renforcer la collaboration opérationnelle par l'intermédiaire de réunions annexes et de discussions stratégiques.

Le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique d'INTERPOL est responsable de l'exécution du projet AFJOC dans le cadre d'un partenariat étroit avec des acteurs régionaux de premier plan, en particulier le mécanisme de coopération policière de l'Union africaine, AFRIPOL, la communauté des services chargés de l'application de la loi et le secteur privé.

Contact

Bureau pour les opérations de lutte contre la cybercriminalité en Afrique
AfricaDesk@interpol.int

INTERPOL

INTERPOL HQ

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ