CELLULE NATIONALE DE TRAITEMENT DES INFORMATIONS FINANCIÈRES

RAPPORT D'ANALYSE STRATÉGIQUE : INDICATEURS ET TENDANCES DE BLANCHIMENT DE CAPITAUX LIÉS À LA CYBERCRIMINALITÉ (2020-2022)

SEPTEMBRE 2023

TABLE DES MATIÈRES

RÉSUME ANALYTIQUE

Le blanchiment des produits de l'infraction est un aspect important à étudier dans la lutte contre la cybercriminalité en Côte d'Ivoire. En effet, les cybercriminels cherchent souvent à dissimuler les produits qu'ils ont obtenus grâce à leurs activités illégales. Ainsi, ils utilisent des techniques sophistiquées pour blanchir l'argent sale, notamment en le transférant à travers différents comptes bancaires et en le dissimulant dans des investissements ou des acquisitions de biens. Ils utilisent également le canal des sociétés de transfert de fonds et de valeurs.

La Cellule Nationale de Traitement des Informations Financières (CENTIF), organisme de renseignement spécialisé dans la lutte contre les circuits financiers clandestins et le blanchiment d'argent, joue un rôle essentiel dans la détection et la prévention de ces activités illicites. Elle apporte aussi sa contribution dans le processus d'identification et de saisie des produits générés par lesdites activités. En travaillant en étroite collaboration avec les institutions financières et les autres autorités nationales, elle peut identifier les transactions suspectes et les comportements inhabituels qui pourraient indiquer une activité de blanchiment de capitaux liée à la cybercriminalité.

En outre, la coopération internationale est par ailleurs cruciale dans la lutte contre le blanchiment de capitaux lié à la cybercriminalité. Les cybercriminels opèrent souvent à l'échelle mondiale, ce qui rend nécessaire une collaboration entre les différentes autorités et les organismes de lutte contre la criminalité dans le monde entier. La CENTIF doit donc partager ses informations et ses connaissances avec d'autres pays et organisations, afin de mettre en place des actions concertées pour démanteler les réseaux de blanchiment d'argent liés à la cybercriminalité.

En résumé, la lutte contre la cybercriminalité et le blanchiment de capitaux en Côte d'Ivoire requiert des mesures multidimensionnelles. Elle nécessite une approche proactive, grâce à la diffusion d'indicateurs permettant de détecter des activités suspectes de blanchiment de capitaux associées à la cybercriminalité, de renforcer la sécurité informatique, de réglementer l'ouverture, l'exploitation et le contrôle des cybercafés. Parallèlement, il est essentiel de combiner les efforts des institutions financières, de la CENTIF, des autorités nationales et internationales pour lutter efficacement contre ces phénomènes criminels et protéger ainsi le pays et ses citoyens de ces menaces croissantes.

INTRODUCTION :

La Côte d'Ivoire est confrontée depuis plusieurs décennies au phénomène de la cybercriminalité. Ce fléau a connu plusieurs développements dont les formes les plus répandues sont : le vol d'identité, l'escroquerie aux sentiments, l'atteinte à la dignité humaine, la fraude sur les transactions qui permet aux délinquants d'obtenir des

informations personnelles et bancaires des victimes, d'accéder à leurs comptes bancaires, d'y subtiliser leur épargne et même contracter des dettes en leur nom.

Avant la création de la CENTIF en 2008, la lutte contre ce type d'infraction n'intégrait pas assez le volet de l'analyse et du circuit financier utilisé par les délinquants. Depuis lors, l'aspect relatif au blanchiment de capitaux a été intégré dans la lutte et semble en devenir l'un des aspects les plus importants. En effet, les criminels utilisent des transactions financières en ligne pour dissimuler l'origine illégale des fonds obtenus. Ils peuvent utiliser des crypto-monnaies comme le Bitcoin pour effectuer des transferts anonymes, et ainsi blanchir des sommes importantes.

Enfin, il est essentiel de mentionner que la cybercriminalité dépasse souvent les frontières nationales, rendant la poursuite et la punition des criminels plus difficiles. Les criminels peuvent utiliser des réseaux de serveurs proxy et des logiciels de cryptage pour dissimuler leur identité et leur localisation, ce qui rend les enquêtes plus complexes.

Face à ce phénomène en croissante évolution, comment améliorer la capacité de détection des transactions suspectes par les professionnels assujettis en matière de cybercriminalité associée au blanchiment de capitaux ?
Comment aider efficacement les autorités d'enquête et de poursuite dans la lutte contre la cybercriminalité et le blanchiment de capitaux ?
Comment accroître l'efficacité de la coopération nationale et internationale relativement à la lutte contre la cybercriminalité et le blanchiment ?
Quelles sont les tendances observées relativement au blanchiment de capitaux associé à la cybercriminalité ? Et comment les diffuser de façon périodique ?

I- CONTEXTE :

La cybercriminalité est devenue l'une des principales menaces intérieures en Côte d'Ivoire, comme le souligne l'Évaluation Nationale des Risques (ENR) publiée en 2019. Cette affirmation est renforcée par une récente étude du Groupe Intergouvernemental de lutte contre le Blanchiment d'Argent en Afrique de l'Ouest(GIABA), qui indique que ce phénomène est répandu dans toute l'Afrique de l'Ouest.

De 2017 à 2021, la CENTIF a enregistré un total de 2306 déclarations d'opérations suspectes, provenant de professionnels assujettis tels que les banques. Parmi ces déclarations, 172 étaient liées à la cybercriminalité. Ce qui représente 13,41 % de l'ensemble de ces communications. Il est intéressant de noter que la plupart des victimes identifiées dans ces dossiers sont d'origine étrangère.

Les déclarations de soupçon relatives à la cybercriminalité ont connu une hausse constante de 2017 à 2019. Mais, cette tendance a commencé à décroître à partir de 2020. Depuis lors, le nombre de déclarations de blanchiment de capitaux associées à la cybercriminalité reste relativement constant.

Par ailleurs, il ressort des données des autorités d'enquête chargées de la lutte contre la cybercriminalité que les efforts déployés par l'État de Côte d'Ivoire pour endiguer le phénomène n'a pas encore permis de réduire le nombre de plaintes ainsi que les préjudices résultant de ce type de délinquance.

La cybercriminalité génère d'importantes sommes, qui sont ensuite blanchies dans divers secteurs. Cette situation a des conséquences néfastes sur le plan social, sécuritaire et économique. Selon les données de la Direction de l'Informatique et des Traces Technologiques (D.I.T.T), de **2016 à 2020**, le préjudice global résultant des plaintes portant sur la cybercriminalité est estimé **23.031.633.449 FCFA**.

L'objectif du présent rapport est d'identifier les tendances en matière de cybercriminalité en Côte d'Ivoire ainsi que les indicateurs de blanchiment de capitaux et de Financement du Terrorisme liés à ce phénomène.

Ces résultats permettront de soutenir les professionnels assujettis à la loi relative à la lutte contre le Blanchiment de capitaux et le Financement du Terrorisme (LBC/FT) dans la mise en œuvre de leurs obligations déclaratives, d'aider les autorités d'enquête et de poursuite à considérer la dimension du blanchiment de capitaux dans la lutte contre cette infraction.

I. MÉTHODOLOGIE :

Ce rapport est une synthèse issue de l'analyse de 55 rapports de disséminations soumis par la CENTIF au parquet du Pôle Pénal Économique et Financier (PPEF) et à la D.I.T.T de 2020 à 2022. Ces disséminations s'articulent autour de 53 déclarations d'opérations suspectes ainsi que de 14 signalements des homologues étrangers.

Il convient de rappeler que les rapports de dissémination, transmis par la CENTIF aux autorités judiciaires, ont été obtenus grâce au traitement des informations provenant surtout de trois sources :

- Les déclarations de soupçon transmises par les professionnels assujettis à la loi relative au BC/FT.
- Les informations fournies par les administrations partenaires de la CENTIF.
- Les transmissions spontanées et les demandes d'informations reçues par la CENTIF des cellules de renseignement financier (CRF) étrangères.

Les données, tant quantitatives que qualitatives, recueillies dans ces rapports de disséminations ont fait l'objet d'une analyse approfondie afin de déterminer avec précision les principaux indicateurs d'alerte et les tendances en matière de blanchiment lié à la cybercriminalité.

Ces différentes analyses ont permis d'obtenir des informations précieuses, notamment concernant les montants en jeu, le profil des cybercriminels, les zones géographiques à risque et la prévalence des formes de cybercriminalités.

II. TENDANCES IDENTIFIÉES :

Dans la période de 2017 et 2022, la Cellule Nationale de Traitement des Informations Financières (CENTIF) a enregistré un total de 191 Déclarations de Soupçon (DOS) en relation avec la cybercriminalité, ce qui représente une moyenne annuelle de 31 DOS. Une tendance à la hausse a été observée de 2017 à 2019. Cependant, à partir de l'année 2020, une baisse du nombre de déclarations par rapport à la moyenne annuelle a été constatée. Cette tendance décroissante s'est poursuivie jusqu'en 2022 (voir tableau 1).

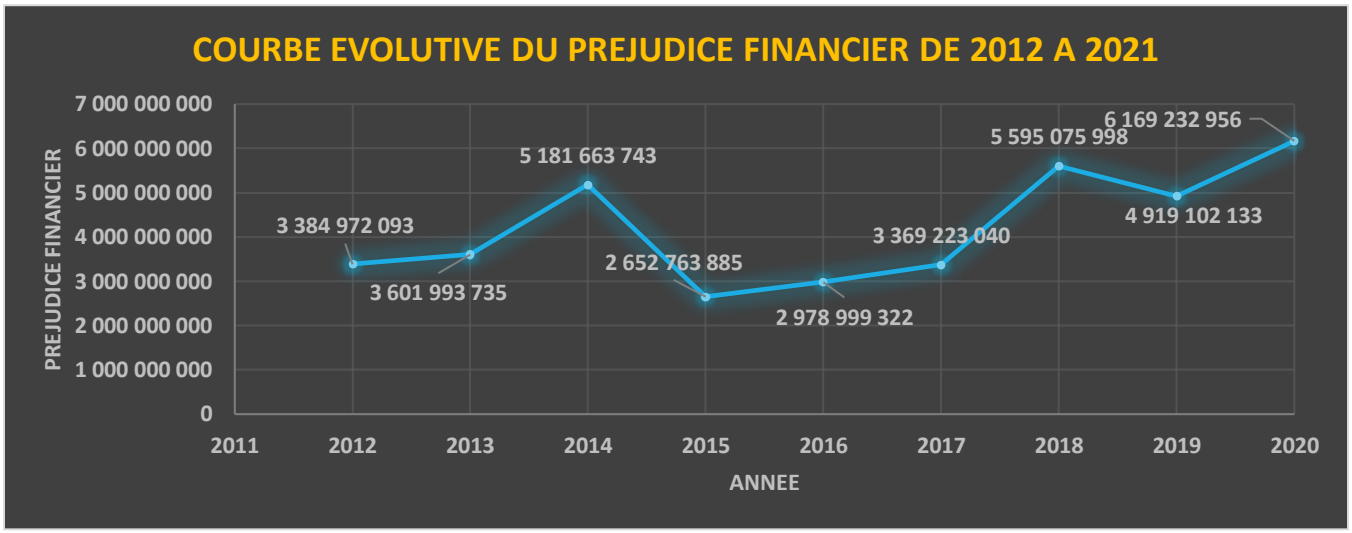
Année	2017	2018	2019	2020	2021	2022	TOTAL
Nombre de DOS de Cybercriminalité	32	35	71	16	18	19	191

Tableau 1 : Nombre de DOS en lien avec la cybercriminalité ***Source : CENTIF-CI***

Le développement de la connectivité Internet a conduit à une croissance notable du nombre de cybercriminels. Selon les données de la D.I.T.T, les infractions liées à la cybercriminalité les plus courantes en Côte d'Ivoire sont : l'escroquerie aux faux sentiments, le chantage vidéo, la fraude sur le porte-monnaie électronique et l'utilisation frauduleuse d'éléments d'identification de personnes physiques ou morales. Des cas concernant les menaces, la pornographie infantile, le piratage, le vol de données, l'organisation de fausses loteries, le détournement de courriers destinés aux banques, les escroqueries à la voiture d'occasion, l'établissement de faux documents officiels, la diffusion de fausses informations, ainsi que la diffamation ou les injures sur Internet ont été également enregistrés.

Concernant le préjudice financier, on observe une progression constante de **2011** à **2020,** année durant laquelle il atteint son point culminant avec un cumul de **6.169.232.956 FCFA**. Cette période correspond à celle de la pandémie de COVID-19, durant laquelle ce type d'infraction a connu une croissance en raison de l'utilisation beaucoup plus fréquente d'internet.

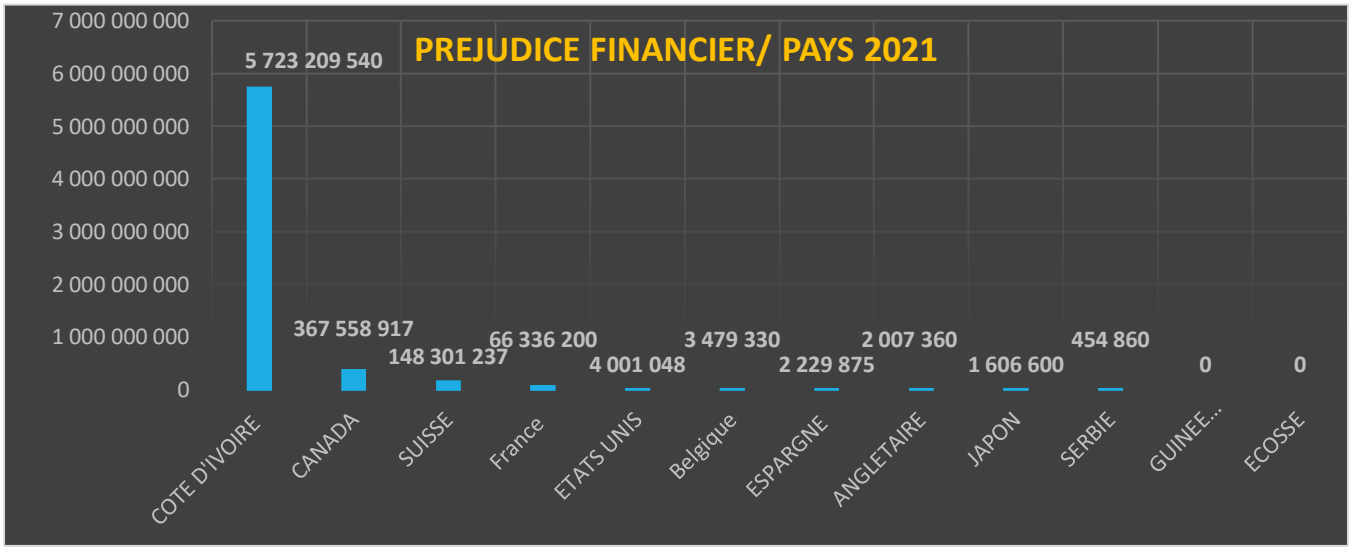
Le préjudice financier le plus bas a été enregistré en 2015 avec un montant cumulé de **2.978.999.322 FCFA** (voir graphique 1).



Graphique 1 : Évolution du préjudice financier des infractions de cybercriminalité de 2011 à 2020

Source : D.I.T.T

Selon les informations fournies par la D.I.T.T, en 2021, les victimes ayant subi le préjudice le plus élevé sont celles qui résident en Côte d'Ivoire avec un chiffre estimé à **5.723.209.504** FCFA. Elles sont suivies par les victimes qui résident au Canada et en Suisse avec respectivement les sommes de **367.558.917 FCFA et 148.301.237 FCFA** (graphique 2).



Graphique 2 : Préjudice financier cybercriminalité par pays en 2021 ***Source : D.I.T.T***

De plus, l'émergence des délits liés aux transactions téléphoniques a été rendue possible par la vulgarisation des moyens de paiement mobiles.

De façon spécifique, la fraude par carte téléphonique a causé un dommage financier **de 926 000 000 de** francs CFA à la Côte d'Ivoire en 2014. La manière d'opérer dans ce type de fraude permet aux délinquants de faire des appels téléphoniques internationaux en contournant les canaux de télécommunications dédiés aux communications internationales. L'objectif étant de minorer les tarifs de ces appels en les faisant passer pour des communications nationales ou locales. Cette fraude a causé d'énormes pertes aux entreprises de télécommunication.

Les schémas identifiés dans le cadre des recherches menées touchent les aspects suivants :

1. Nombre de disséminations et les autorités compétentes récipiendaires :

Durant l'intervalle de temps examiné, la CENTIF a procédé à la diffusion de 55 rapports de dissémination à l'attention des autorités compétentes, en particulier les autorités judiciaires (35) et les autorités d'enquête (20). Ces rapports ont été obtenus à la suite de l'analyse de 53 déclarations d'opérations suspectes soumises principalement par les assujettis du secteur bancaire, de déclarations systématiques de transactions en espèces et de (14) signalements d'homologues étrangers en lien avec la cybercriminalité.

Ces communications mettent en cause aussi bien des personnes physiques que morales clientes des banques et des sociétés de transfert rapide d'argent, agissant comme sous-agents agréés.

Toutefois, il convient de noter que la CENTIF a reçu un nombre limité de demandes d'informations de la part des autorités d'enquêtes spécialisées en matière de cybercriminalité. En outre, elle n'a pas reçu de retour d'information sur les notes transmises à la D.I.T.T de façon spécifique.

2. Secteurs impliqués (incluant le type de produit concerné dans les cas de BC/FT) :

L'analyse des cas a révélé certains domaines d'activités de prédilection des cybercriminels, notamment celui des services, avec une préférence pour le commerce en général. La grande majorité des cybercriminels déclarent mener une activité commerciale, surtout dans le domaine de l'achat, la vente et la location de véhicules, la vente de téléphones portables. Cependant, dans la plupart des cas examinés, les déclarants n'ont pas systématiquement exigé la présentation d'un registre de commerce pour attester de l'activité déclarée du client présumé impliqué dans la cybercriminalité. Ils se sont

simplement contentés de la déclaration du client, sans procéder à une vérification, avant, au cours ou même après l'entrée en relation d'affaires.

Cela soulève des interrogations quant à la réalité des activités déclarées par les clients et la possibilité d'utiliser celles-ci comme une couverture pour s'adonner à des activités illégales.
Les cybercriminels déclarent en général au professionnel assujetti des activités à fort potentiel d'utilisation d'espèces ou des activités nécessitant des relations avec l'extérieur, notamment l'achat et la vente de véhicules.

3. Montants impliqués dans les disséminations :

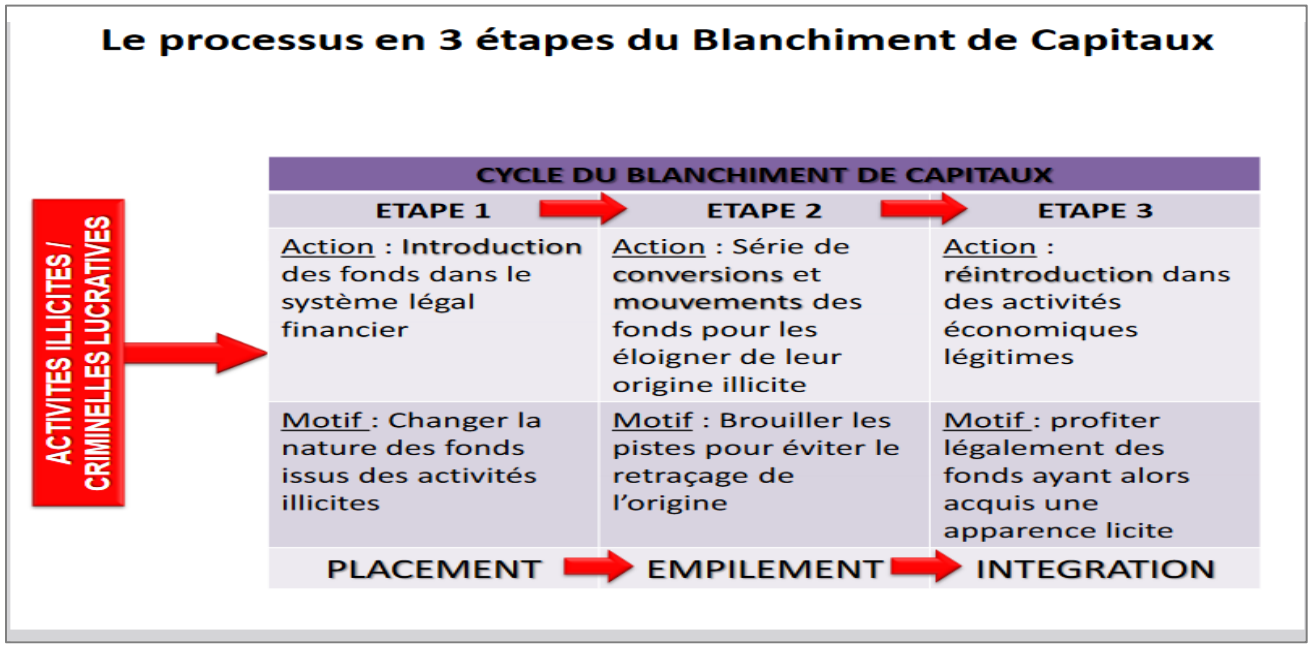
Les dossiers de dissémination comportent des informations sur les montants impliqués dans les infractions liées à la cybercriminalité. Cependant, il convient de noter que les montants rapportés dans ces dossiers ne constituent qu'une partie de l'activité de cybercriminalité, car de nombreux cas de ce type d'infractions ne sont ni signalées ni identifiées. De plus, les montants réels peuvent être sous-estimés ou surestimés en fonction des informations disponibles.

Il est également important de souligner que les activités de cybercriminalité sont en constante évolution et que de nouvelles formes d'infractions émergentes régulièrement. Par conséquent, il est difficile d'évaluer en particulier le montant total du produit de la cybercriminalité, car cela nécessiterait une surveillance continue et une analyse approfondie des tendances et des méthodes utilisées par les cybercriminels.

L'analyse des données de 2020 à 2022, révèle que les agissements des cybercriminels depuis le territoire ivoirien ont porté un préjudice financier cumulé estimé à **13. 865. 723. 745 FCFA**, soit **23. 445. 691 USD** ou **21. 138 .157 euros** aux ressortissants étrangers**.**
Ces chiffres soulignent l'ampleur des activités criminelles en ligne perpétrées depuis la Côte d'Ivoire et les préjudices financiers considérables subis par les victimes étrangères.

4. Phases du blanchiment de capitaux dans les dossiers de cybercriminalité :

De manière traditionnelle, le processus de blanchiment d'argent se fait en trois étapes (voir graphique 3) :



Graphique 3 : Les étapes du blanchiment

Lors de notre analyse, il est apparu que la phase de placement, qui consiste à introduire des fonds illicites dans le système bancaire, se confondait souvent avec la consommation de l'infraction de cybercriminalité.

Cependant, puisque les fonds sont retirés après le transfert par les victimes, nous pouvons considérer qu'ils sont blanchis dès le placement. En effet, le système bancaire lui-même est utilisé comme instrument pour commettre l'infraction. En effet, les cybercriminels ouvrent des comptes bancaires dans le seul but de recevoir les produits de leurs escroqueries. Dans l'hypothèse où les fonds seraient retirés en espèces, on peut en déduire que nous sommes à l'étape du placement.

Dans la grande majorité des cas, les déclarations des assujettis étaient faites après le retrait de l'ensemble des fonds par les cybercriminels. Cela pourrait signifier que les déclarations sont généralement faites au minimum au stade du placement des fonds, voire de l'empilage. En effet, les cybercriminels étant en possession du produit du délit, ils peuvent l'utiliser pour acquérir des biens de consommation ou investir dans l'économie formelle (empilage et intégration).

Dans bien des cas, les déclarations de soupçon faites sans délais au stade du placement ont fait l'objet d'oppositions de la part de la CENTIF, en raison de la disponibilité des fonds sur les comptes bancaires.

5. Indicateurs communs de BC/FT :

Les dossiers de cybercriminalité ont révélé que les motivations derrière ces actes sont également variées.

Certains cybercriminels cherchent à obtenir un gain financier en volant des informations personnelles ou bancaires, en effectuant des escroqueries en ligne ou en exigeant des rançons pour débloquer des données.

D'autres cherchent simplement à causer des préjudices, à perturber des systèmes informatiques ou à violer la vie privée d'autrui.

Les cybercriminels peuvent agir de façon solitaire, comme hackers individuels ou comme membres d'un groupe organisé. Certains groupes de cybercriminels sont très sophistiqués et bien organisés, avec des compétences techniques avancées et une connaissance approfondie des systèmes informatiques et des réseaux.

L'analyse des dossiers reçus dans le cadre de cette étude a permis de repérer, à partir des informations qu'ils contenaient, les indicateurs communs qui ont contribué à dresser le profil et à déterminer les méthodes d'action adoptées par les cybercriminels.

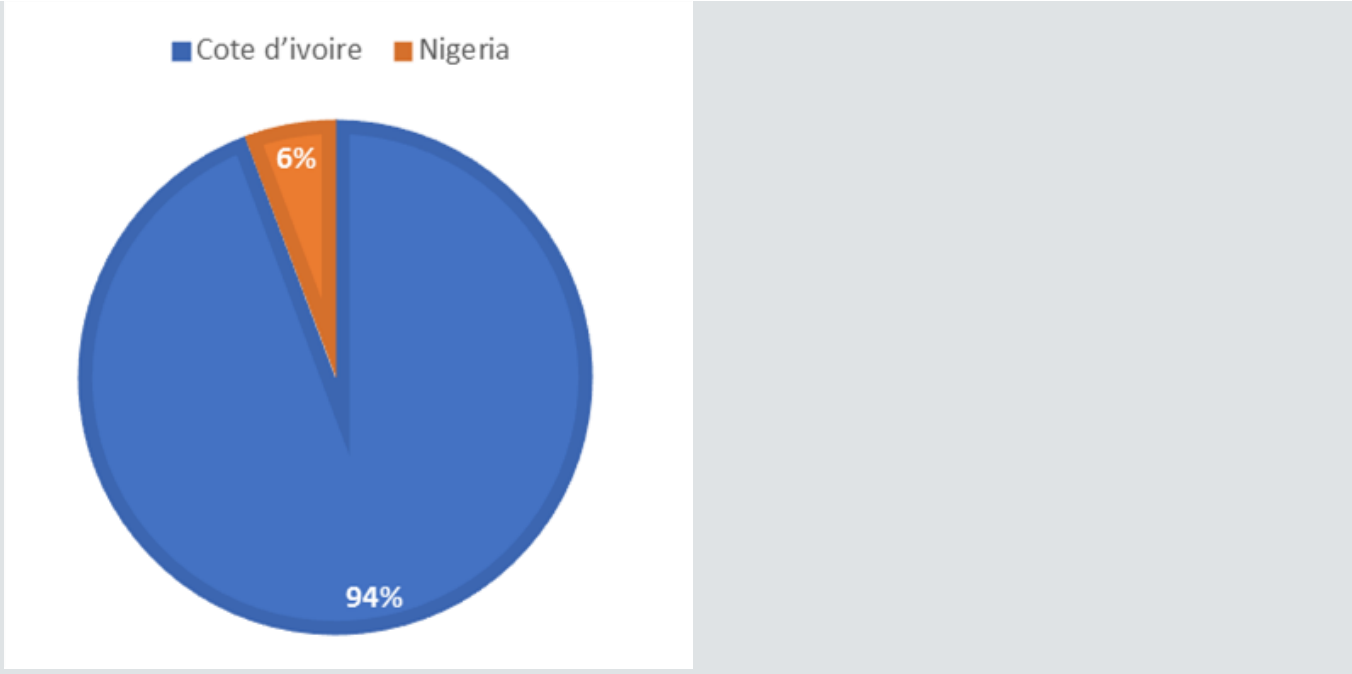
5.1. Indicateurs liés au profil des auteurs des actes de cybercriminalité :

L'étude du profil des individus impliqués dans des actes de cybercriminalité suscite des interrogations quant à leur véritable identité et à l'activité qu'ils mènent. En réalité, ils prétendent successivement être des commerçants prospères, des hommes d'affaires influents ou des étudiants. En général, ils sont âgés de 18 à 35 ans.

ANNÉE DE NAISSANCE	**1985**	**1986**	**1970**	**1972**	**1984**	**1987**	**1988**	**1989**	**1990**	**1991**	**1992**	**1993**	**1994**	**1995**	**1996**	**1997**
NOMBRE DE PERSONNES	**2**	**1**	**1**	**1**	**1**	**2**	**2**	**3**	**3**	**8**	**5**	**2**	**13**	**1**	**5**	**1**

Tableau 2 : Répartition de cybercriminels par année de naissance

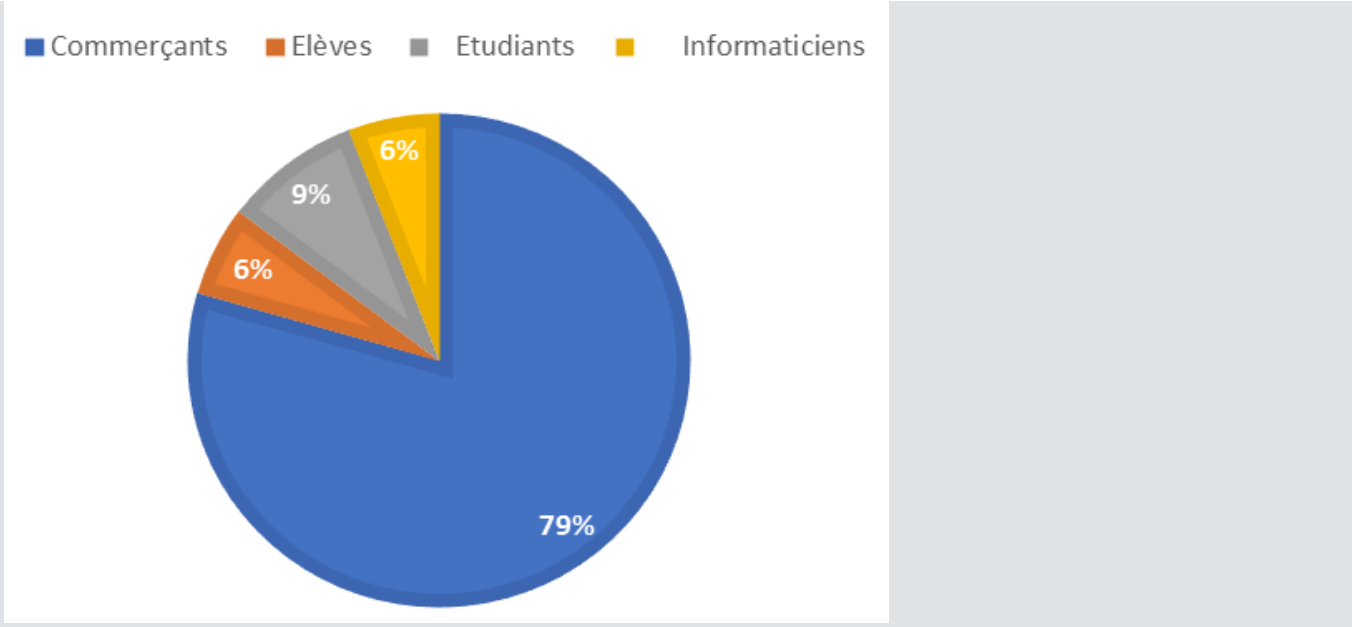
La grande majorité des individus impliqués dans des crimes informatiques et opérants à partir du territoire ivoirien sont des nationaux. Ils représentent 94 % de l'ensemble des auteurs, tandis que les ressortissants étrangers, principalement de nationalité nigériane, représentent à peine 6 % (voir graphique 5).



Graphique 5 : Répartition de cybercriminels par nationalité

Les cybercriminels ivoiriens sont souvent impliqués dans des escroqueries en ligne telles que l'escroquerie aux sentiments, l'usurpation d'identité, le phishing ou l'hameçonnage. Cette dernière est une forme d'escroquerie qui consiste à obtenir du destinataire d'un courriel ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent. Le fraudeur se fait passer pour un organisme officiel, par exemple, une banque ou un service des impôts. Le piratage de comptes bancaires et le vol de données personnelles. Ils ciblent principalement des personnes résidant à l'étranger, car ces victimes sont généralement perçues comme plus riches et moins méfiantes.

L'objectif des cybercriminels ivoiriens est d'obtenir de l'argent rapidement et en toute impunité. Ils utilisent des techniques sophistiquées pour tromper leurs victimes, notamment en se faisant passer pour de potentiels partenaires amoureux ou des organisations reconnues. Une fois qu'ils ont gagné la confiance de leurs victimes, ils les persuadent souvent de leur envoyer de l'argent sous la menace de divulgation des informations personnelles sensibles. Ils peuvent également infecter les ordinateurs de leurs victimes avec des logiciels malveillants pour voler des informations bancaires ou d'autres données sensibles afin de réaliser des fraudes à la carte bancaire.



Graphique 6 : Répartition cybercriminels par profession

La principale motivation des cybercriminels ivoiriens est surtout l'enrichissement illicite. Les opérations de retraits systématiques des fonds ainsi que leurs origines donnent l'impression qu'ils sont motivés par l'opportunité de gagner rapidement de l'argent sans risque apparent, grâce à l'anonymat et à la complexité que procure le cyberespace. En outre, le faible niveau de sensibilisation aux risques liés à la cybercriminalité en Côte d'Ivoire pourrait faciliter les activités des cybercriminels. De nombreuses personnes ne sont pas conscientes des dangers potentiels que pourrait représenter la connexion à un réseau en ligne et ne prennent pas les dispositions requises pour protéger leurs informations personnelles et financières. Enfin, la perception de l'impunité pourrait également motiver les cybercriminels ivoiriens à poursuivre leur crime.

En raison des difficultés pour certaines victimes à porter plainte et pour les autorités à enquêter et à poursuivre tous les auteurs, les cybercriminels peuvent se sentir en sécurité et continuer à commettre leurs méfaits sans craindre d'être arrêtés ou punis.

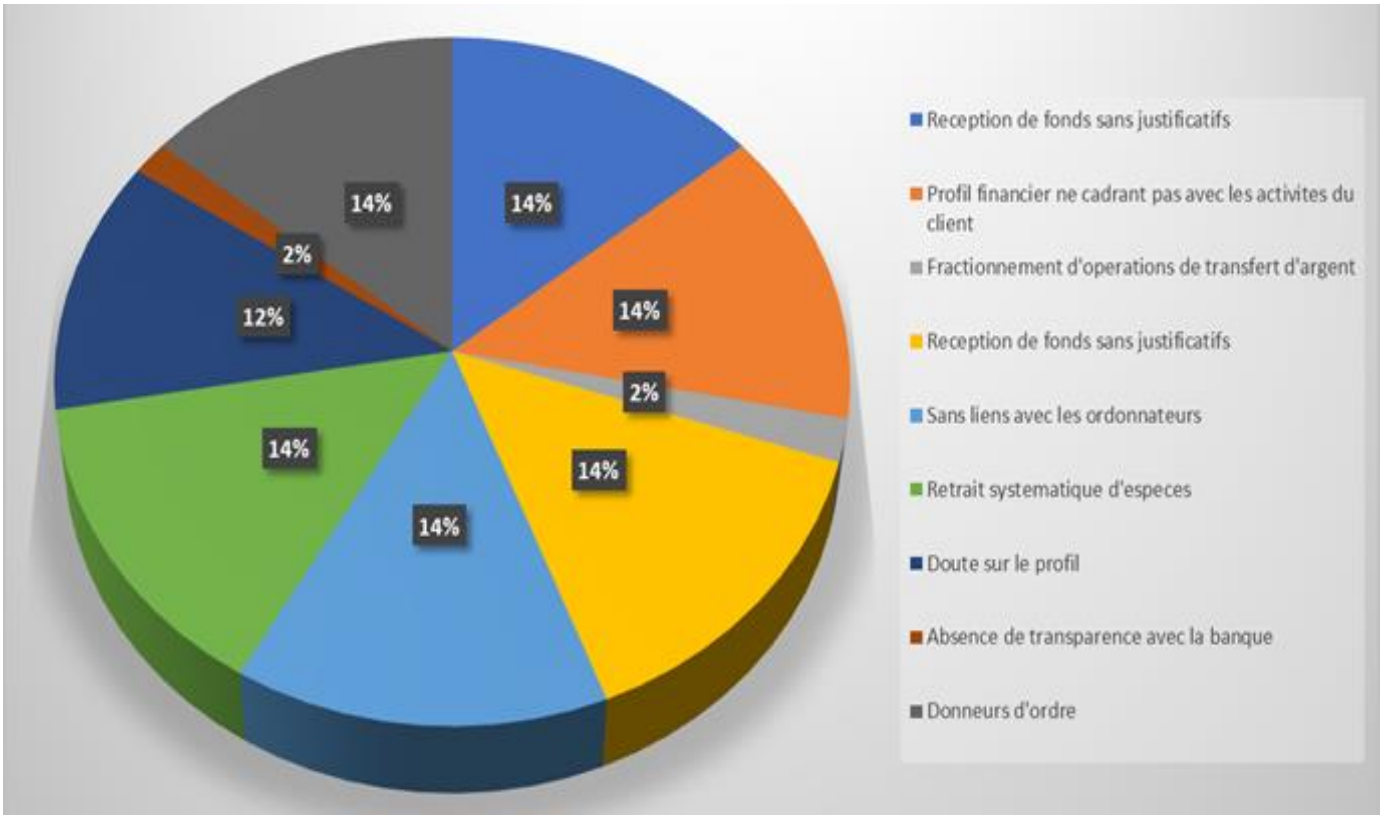
5.2. Autres indicateurs :

Indicateurs de risque relatifs à l'identité du client	**Indicateurs de risque relatifs aux fonds et aux comptes**
Refus de communication de certains documents d'identification	Multiples transactions de retraits en espèces de façon systématique via le Distributeur Automatique de Billets (DAB) ou à la Caisse

Indicateurs de risque relatifs à l'identité du client	Indicateurs de risque relatifs aux fonds et aux comptes
Documents d'identification incomplets, incohérents, insuffisants ou falsifiés	Inadéquation entre les transactions sur le compte et le profil du client
Dissimulation de l'identité du bénéficiaire effectif	Motifs communiqués non conformes aux transactions
Dissimulation de l'origine des fonds par le client	Fonds provenant de juridictions à risque
Doutes sur les liens entre le donneur d'ordre et le client	Absence de virement de salaire, ou de versement recettes d'activités commerciales sur le compte
Client ayant des antécédents criminels	Absence de lien entre le bénéficiaire des opérations et le donneur d'ordre
Profil ne cadrant pas avec l'activité déclarée lors de l'ouverture du compte	Solde du compte toujours débiteur une fois les virements réceptionnés
Doute sur l'activité réelle du client	Succession de transferts et des retraits sur une courte période définie
Réception en peu de temps de plusieurs virements de l'étranger	Changements fréquents des mandataires ou des personnes qui alimentent le compte du client
Personne habitant une zone identifiée comme zone de prédilection de cybercriminels (voir section 7)	Compte alimenté uniquement par des fonds en provenance de l'étranger.
Refus ou difficultés du client à fournir les renseignements demandés lors de l'ouverture du compte	Inadéquation entre les transactions et le profil du compte.
Client utilisant des noms différents d'une opération à l'autre ou des « alias »	Transfert systématique des produits des transactions à un tiers
Adresses et numéros de téléphone identiques utilisés par plusieurs clients qui ne semblent pas être liés	Transferts fréquents de fonds en provenance de l'étranger sur un compte dormant
Client faisant preuve d'un comportement nerveux	Reprise soudaine des activités sur des comptes inactifs
Explication insuffisante sur l'origine des fonds	Détention ou gestion de comptes multiples par un seul client ou une seule personne
Client qui ferme le compte après qu'un dépôt ou virement initial a été effectué sans explication appropriée	Fermeture brusque et injustifiée du compte par le client
Opérations financières atypiques par rapport au profil financier du client	Patrimoine non justifié ne correspondant pas à la situation économique du client

Indicateurs de risque relatifs à l'identité du client	Indicateurs de risque relatifs aux fonds et aux comptes
Activité transactionnelle (niveau ou volume) en inadéquation avec la situation financière apparente du client, le modèle économique habituel de l'activité exercée ou avec le profil professionnel (étudiant, chômeur, coiffeuse, informaticien, etc.)	L'alimentation continue d'un compte au-delà du revenu déclaré
Le Client semble vivre au-dessus de ses moyens.	Client en lien avec des juridictions non coopératives en termes de LBC/FT
	Compte avec un faible volume de transactions qui reçoit ou transfère un montant important
	Client qui effectue des modalités complexes de décaissements sur le compte

Il ressort de l'analyse que les indicateurs les plus probables sont : la réception de fonds sans justificatif, absence de lien avec le donneur d'ordre, profil financier ne cadrant pas avec les activités déclarées du client, retirait systématique d'espèces dès la réception des fonds. (Voir graphique 7).



Graphique 7 : Indicateurs de cybercriminalité

6. Infractions sous-jacentes :

Quelques types de cybercriminalités en Côte d'Ivoire :

6.1. Escroquerie relative aux offres d'emploi :

Les arnaques liées aux offres d'emploi constituent une manœuvre frauduleuse dans laquelle la personne trompée reçoit une correspondance non sollicitée lui proposant un poste, généralement en dehors de son domaine de compétence. Lorsque ladite personne ouvre le courrier et consent à suivre les instructions fournies par le biais du courrier électronique, elle se voit déposséder de ses données personnelles. Ces informations seront ultérieurement exploitées par le cybercriminel, à son insu, afin d'escroquer ou d'extorquer de l'argent.

6.2. Escroquerie à la loterie :

Suivant ce mode opératoire, la victime est contactée par courrier électronique et informée qu'elle a gagné une importante somme à la loterie. Paradoxalement, il lui est demandé de fournir ses données personnelles pour vérification ainsi qu'un acompte ou une avance modique avant d'entrer en possession de ses gains. Une fois ces démarches accomplies, la victime perd brusquement tout contact avec l'expéditeur du courrier électronique qui lui aura simultanément extorqué de l'argent et usurpé son identité.

6.3. Escroquerie aux bénéficiaires :

Dans cette situation particulière, la personne victime reçoit une correspondance électronique qui provient d'un individu cherchant à effectuer un transfert d'argent de manière urgente. Ces courriels proviennent souvent de personnes prétendant faire partie d'une famille royale ou souhaitant léguer leurs biens, voire affirmant posséder des sommes colossales qu'elles désirent faire sortir d'un pays. Ces individus demandent l'assistance de la victime en contrepartie des futurs gains substantiels. L'expéditeur fournit juste assez de détails pour donner une apparence légitime à cette proposition.

Cependant, les fonds promis sont systématiquement retardés pour une série de motifs fallacieux invoqués par le donneur d'ordre, qui incite la victime à avancer divers frais afin de faciliter le transfert des fonds.

6.4. Escroquerie au mariage ou arnaque aux sentiments :

Les individus malveillants élaborent de faux profils sur les plateformes de médias sociaux et les sites de rencontres en ligne. Ces actions visent à cibler des personnes et à simuler une passion amoureuse pour obtenir des avantages financiers de leur part.

Mode opératoire :

L'escroc, de sexe masculin ou féminin, opère sur Internet sous une fausse identité et entre en contact avec sa victime, par exemple, via Facebook. Les échanges débutent par des conversations banales, au cours desquelles les deux parties se dévoilent mutuellement, puis rapidement, l'escroc prétend éprouver des sentiments amoureux. Si la victime se laisse éblouir, elle tombe dans une spirale de promesses non tenues qui alternent avec des demandes financières. Pendant des semaines, voire des mois, la prétendue relation amoureuse se construit via des applications telles que Skype, WhatsApp, etc. Souvent, l'escroc prétend être confronté à des difficultés financières dues à des problèmes de santé graves ou affirme être sur le point de recevoir un héritage important. Il sollicite des fonds de la victime pour des soins médicaux ou pour des démarches administratives en vue de bénéficier de l'héritage, promettant une récompense substantielle en retour. Entre-temps, des projets sont proposés à la victime. Lorsque les fonds sont remis par la victime, un autre problème est avancé par l'escroc pour soutirer encore des fonds, jusqu'à ce que la victime soit ruinée ou prenne conscience de la supercherie.

7. Analyse géographique :

7.1. Sur les environnements favorables ou zones géographiques où prospère la cybercriminalité :

Les délinquants tirent parti des vulnérabilités environnementales en choisissant des lieux où la surveillance des autorités chargées de l'application de la loi n'est pas adéquate, voire inexistante. Par conséquent, ils évitent d'agir depuis leur domicile avec leurs propres outils (ordinateurs et téléphones portables) de peur d'être identifiés grâce à leurs adresses IP. Ils préfèrent mener leurs activités dans des zones géographiques à forte concentration urbaine étudiante où l'accès à internet est aisé (faible débit et nombreux cybercafés). De même, les cybercriminels préfèrent également les banlieues et les zones rurales.

Banlieues :

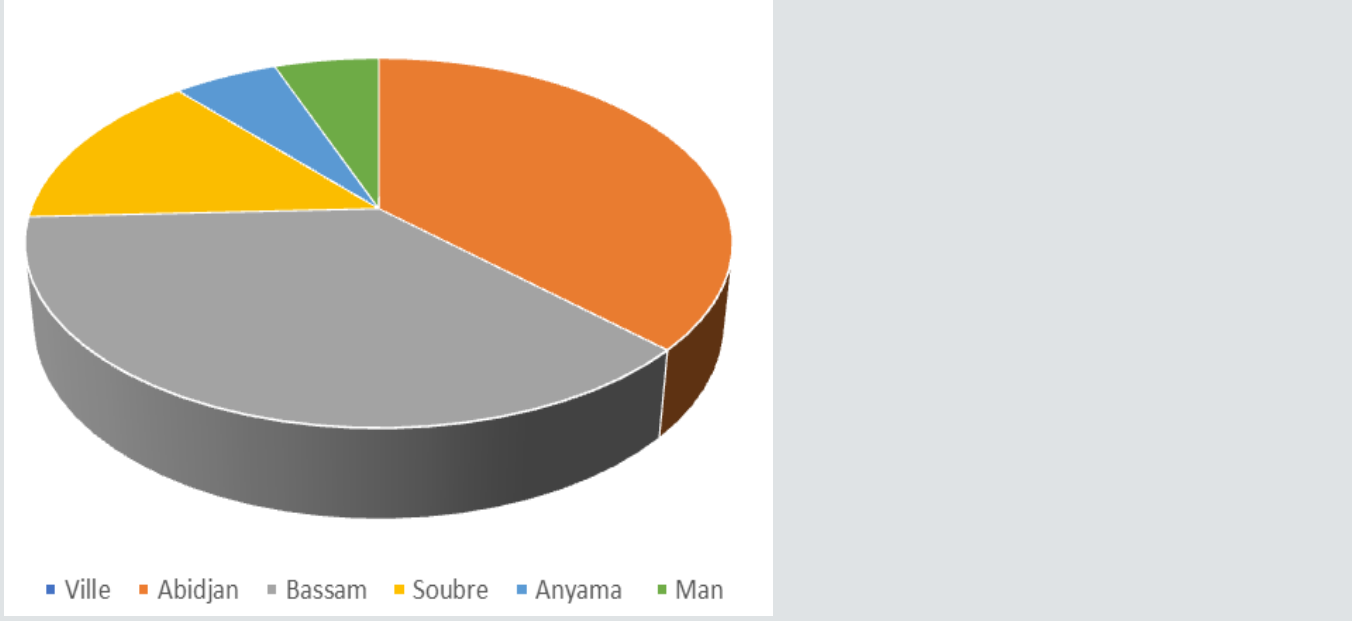
Il ressort que Grand-Bassam cité balnéaire située dans le sud-est de la Côte d'Ivoire, à environ 30 km de la ville d'Abidjan, a enregistré 37 % des cas de cybercriminalité, ainsi que la ville d'Anyama, située à 10 km au nord d'Abidjan qui a connu 08 % des cas.

Zones rurales :

La ville de Soubré située dans la partie sud-ouest du district de Bas-Sassandra du pays, classée au 10e rang des villes les plus peuplées de la Côte d'Ivoire et renommée pour sa production de cacao, fait partie des zones rurales où sévissent les cybercriminels. De même que la ville Man située à l'ouest de la Côte d'Ivoire, capitale administrative du district des Montagnes et de la région du Tonkpi. (Voir graphique 8).

Quartiers peuplés :

En outre, dans la grande commune d'Abidjan, les communes les plus affectées par le phénomène de la cybercriminalité sont Yopougon, Marcory, Treichville, Koumassi et Abobo.
Il s'agit de cités densément peuplées, où l'on trouve de nombreuses activités, où la couverture sécuritaire relativement inadéquate.



Graphique 8 : Répartition cybercriminels par zone géographique

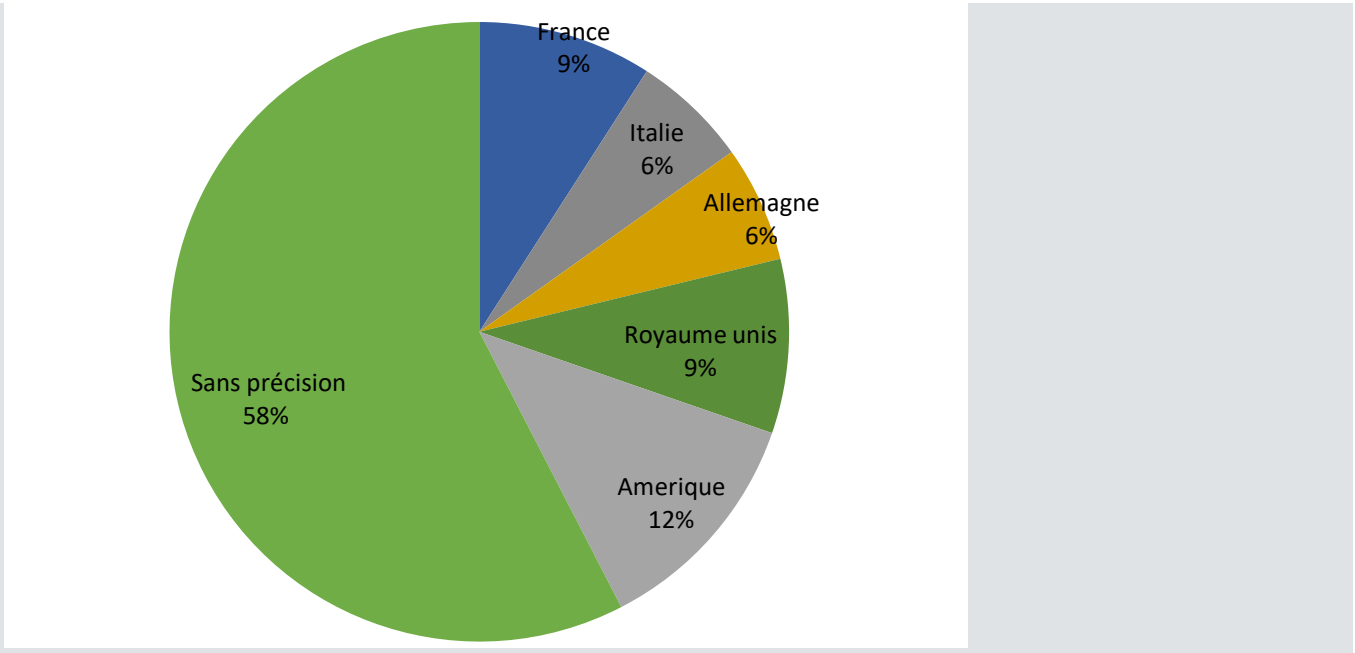
Divers éléments concourent à l'établissement d'un contexte propice à la prospérité des délinquants virtuels, en engendrant ainsi une multitude de personnes susceptibles d'être victimes de leurs méfaits.

7.2. Nationalité des personnes d'intérêt :

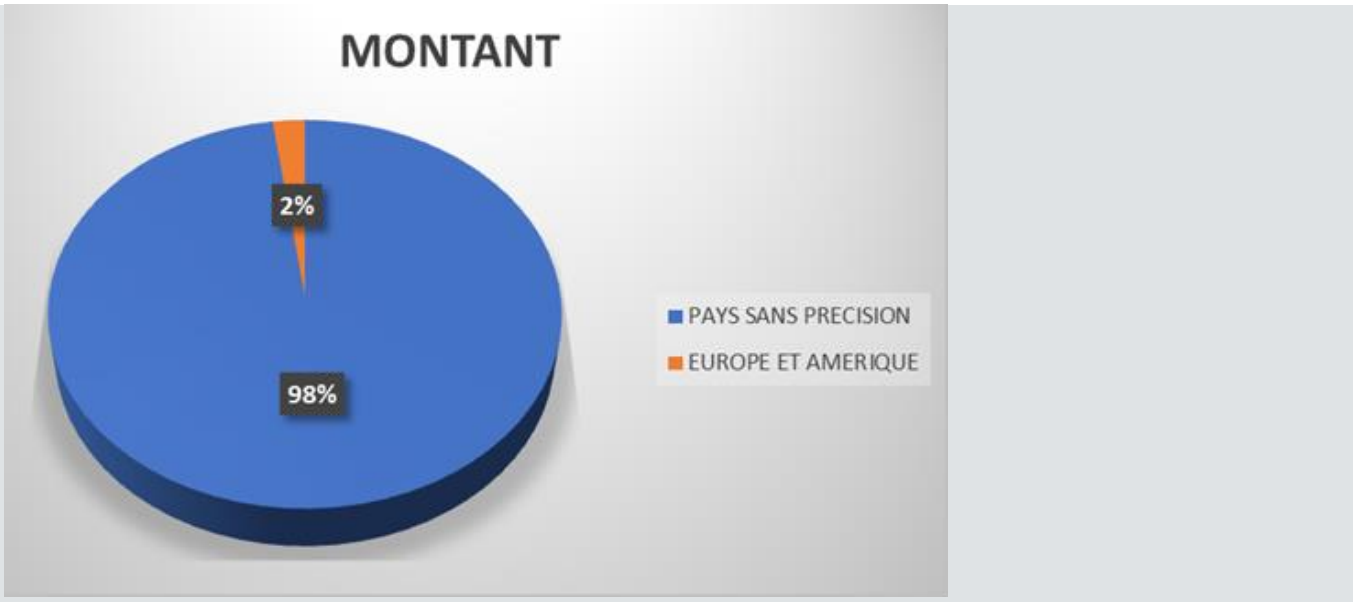
Les individus malveillants résidents en Côte d'Ivoire ciblent également des ressortissants étrangers, notamment de nationalités européennes et américaines. L'analyse révèle que les victimes profilées sont des personnes seules en quête d'affection ou d'une relation durable.

7.3. Pays d'origine des fonds :

L'étude des rapports disséminés indique que les fonds envoyés vers la Côte d'Ivoire proviennent de différents pays. Les informations communiquées révèlent l'Europe comme zone de provenance des fonds transférés. Ainsi, dans onze (11) dossiers, l'Europe est la zone géographique d'origine des virements reçus, dont trois (03) en provenance de la France, deux (02) de l'Italie, deux (02) de l'Allemagne, deux (02) du Royaume-Uni, et deux (02) cas pour lesquels la zone européenne n'est pas indiquée avec exactitude. Ensuite, l'Amérique du Nord avec quatre (04) dossiers, dont trois (03) transferts en provenance des États-Unis d'Amérique, et un dossier (0) du Canada. Il convient de noter que dans dix-sept (17) dossiers, les zones géographiques de provenance des fonds n'ont pas été indiquées. (Voir graphique 9).



Graphique 9 : Répartition d'origine des fonds reçus par les cybercriminels



<u>Graphique 10</u> : Répartition selon le montant des fonds

Lorsqu'ils sont en possession des fonds provenant d'activités criminelles, ces individus mettent en œuvre avec astuce des actions visant à éliminer tout indice permettant d'établir un lien avec leurs méfaits. Ces délinquants font transiter les sommes reçues par le biais de leurs comptes bancaires ou des comptes bancaires de complices qu'ils contrôlent. Ils retirent l'argent aux distributeurs automatiques de billets. S'ils souhaitent éviter les institutions financières traditionnelles telles que les banques, ils optent pour les services de transfert rapide d'argent. L'analyse révèle que cette alternative a été utilisée dans environ 5,8 % des cas étudiés.

1.1. <u>Pays destinataires des fonds :</u>

Les cybercriminels ivoiriens sont perpétuellement à la recherche de moyens faciles, rapides et sûrs pour prendre possession des fonds provenant de leurs activités illégales. Il a été observé dans certains cas que ces individus avaient créé des sociétés de transferts d'argent rapide en vue d'obtenir des agréments de sous-agents auprès des établissements d'institutions financières. Cette autorisation leur permettait d'utiliser lesdites sociétés comme véhicule pour retirer avec des documents d'identité manifestement falsifiés plus aisément leurs avoirs criminels. Ces services d'envoi et de réception de fonds dont les plateformes sont utilisées sont connus sur le plan national et international. Il s'agit notamment des services d'envoi et de réception rapide d'argent, tels que Western Union, RIA ou encore MoneyGram. Cependant, les restrictions imposées par ces services, notamment une limite hebdomadaire de 2 millions et mensuelle de 10 millions pour les montants envoyés, obligent les délinquants à opter dans la majorité des cas à posséder un compte bancaire où ils peuvent domicilier ou à faire transiter des sommes plus importantes.

Cas anonyme 1

Courant 2019, les nommés X, Y, Z, AB, CD et 64 autres individus, agissant visiblement en bande organisée, ouvraient des comptes bancaires, en déclarant qu'ils seraient alimentés par les revenus tirés de leurs activités respectives.
Cependant, les comptes n'étaient principalement crédités que par de multiples transferts de fonds. Ces opérations étaient réalisées à partir de cartes de crédit, dont les titulaires se trouvaient dans des pays étrangers.
Les sommes ainsi reçues sur une période de quatre mois, s'élevaient **à 943. 200. 060 FCFA**.
Les investigations n'ont pas permis d'identifier les liens existants entre les mis en cause et les différents titulaires des cartes débitées. Par ailleurs, certaines victimes avaient demandé à l'institution bancaire la rétrocession de leurs fonds. De plus, les sommes perçues sur le compte étaient systématiquement retirées en espèces.
En outre, comme les transferts reçus, les opérations de débits se faisaient plusieurs fois dans la même journée.

Des hausses de retraits d'espèces sur les comptes des clients de cette banque avaient en particulier été observées, surtout durant un week-end du mois d'avril de la même année. À l'issue de toutes ces opérations, les soldes de la grande partie des comptes bénéficiaires des transferts de fonds étaient quasiment insignifiants eu égard aux retraits massifs des fonds transférés par les victimes.
Ce mode opératoire correspond manifestement à la typologie des infractions d'escroquerie commises par le biais d'internet. Il s'ensuit que, par des manœuvres frauduleuses, les mis en cause seraient parvenus à convaincre des victimes de leur transférer des fonds qu'ils ont reçus. Grâce à ces moyens, ils ont pu escroquer tout ou une partie de leurs biens. Ils auraient également pu obtenir les données bancaires afin de leur soutirer des fonds. Il est probable que les victimes aient fait l'objet de vols de leurs données bancaires sur leur territoire par des complices des escrocs résidents en Côte d'Ivoire. Que ces données aient été transmises à ces derniers qui les ont utilisées.
En procédant comme ainsi, notamment en détenant, manipulant, des fonds qu'ils ont perçus, en vue d'en déguiser l'origine illicite, X, Y, Z, AB, CD et 64 autres ont commis l'infraction de blanchiment de capitaux.
Ce cas a fait l'objet d'une déclaration de soupçon, qui après analyse, a fait l'objet d'une dissémination auprès des autorités judiciaires.

Indicateurs de blanchiment :

1. Comptes bancaires alimentés par de multiples transferts de fonds réalisés à partir de cartes de crédits dont les titulaires se trouvent à l'étranger

2. Retraits systématiques des fonds dès leur réception
3. Volume transactionnel atypique de ces comptes les week-ends
4. Absence de lien entre les mis en cause et les titulaires des cartes de crédit

Cas anonyme 2

Le nommé AC, commerçant, ouvrait un compte chèque en vue d'y domicilier ses revenus. Il n'avait pas précisé à la banque qu'il était en attente de virements en provenance de l'étranger. Cependant, celle-ci constatait, après quelques mois, que le compte commençait à recevoir plusieurs transferts de fonds, émis par divers donneurs d'ordre domiciliés dans des pays étrangers. Ainsi, du 28/08/2013 au 08/04/2019, le compte avait reçu au total (131) opérations de transferts de fonds dont le cumul s'élevait à 953.888.436 FCFA.
Ces transferts n'avaient apparemment aucun lien avec son profil et le nommé AC procédait aux retraits systématiques en espèces de ces fonds, dès qu'ils étaient disponibles sur le compte.
L'enquête n'avait pas pu déterminer à quoi les sommes retirées avaient réellement servi.
Lorsque l'établissement bancaire demandait au titulaire du compte de produire des pièces justificatives des opérations, il en était incapable malgré les multiples relances.

Indicateurs de blanchiment :

1- Non-indication de la provenance des revenus potentiels alimentant le compte pendant l'ouverture ;
2- Compte alimenté par des virements de fonds en provenance de l'étranger alors que le client n'avait pas prévenu la banque à l'ouverture du compte ;
3- Absence de liens apparents entre le bénéficiaire et les donneurs d'ordre ;
4- Non-production de justificatifs économiques relatifs aux virements en provenance de l'étranger.

Cas anonyme 3

Monsieur ENJ, se disant étudiant stagiaire, a ouvert un compte d'épargne dans une banque locale en 2016, dans le but d'y déposer ses économies estimées à 100. 000 FCFA par mois. Ce compte ouvert avec un dépôt initial de 70.000 FCFA est resté inactif jusqu'au 15/12/2020. Quatre ans plus tard, il reçoit, de façon soudaine, un virement de 11.807.226 FCFA en provenance de l'étranger.
Interrogé sur l'origine des fonds, le sujet, dont le profil est en inadéquation avec cette opération, présente un document qui ne semble pas être un courrier authentique. La lettre

en elle-même, tant dans sa forme que dans son contenu, n'était pas conforme aux normes d'un courrier formel. Elle était rédigée avec un niveau de langue approximatif.
En outre, il n'y avait aucun lien visible entre l'expéditeur et le sujet, qui n'a pu non plus justifier le transfert.
Tous ces éléments étaient révélateurs de manœuvres frauduleuses auxquelles s'était livré cet individu sur internet en vue de se faire remettre des fonds par sa victime.

Indicateurs de blanchiment:

1. Inadéquation entre le profil du titulaire du compte et la transaction ;
2. Impossibilité de fournir les motifs économiques de la transaction ;
3. Absence de lien entre le bénéficiaire et donneur d'ordre du transfert ;
4. Activation soudaine d'un compte dormant par des virements reçus de l'étranger

RECOMMANDATIONS :

La cybercriminalité est devenue un problème international et évolutif, y compris en Côte d'Ivoire, comme le souligne ce rapport. Malgré les actions combinées de sensibilisation et de répression, les cybercriminels ont réussi à escroquer un montant estimé de plus de 13 milliards de francs de 2020 à 2022. C'est pourquoi, il est important de sécuriser le cyberespace ivoirien.

Pour lutter contre ce fléau, il est recommandé :

À la CENTIF de:

1- Communiquer de façon périodique aux assujettis, aux autorités d'enquêtes et de poursuite des indicateurs pertinents de blanchiment du produit de la cybercriminalité ;
2- Mettre en place un mécanisme de retour d'information après disséminations à l'endroit des autorités compétentes ;
3- Accroître le nombre de diffusions à l'endroit des autorités d'enquête ;
4- Mettre en place un mécanisme d'échange d'information et de coopération avec les autorités chargées de la répression de la cybercriminalité tant sur le plan national qu'international.

Aux institutions financières de:

1- Renforcer les mesures de vigilance en recherchant les indicateurs d'alerte dans les transactions et dans l'attitude des clients tels que le manque de sérénité, l'empressement anormal et les indicateurs liés à l'identité du client ;
2- Renforcer les mesures de KYC et d'identification, en particulier pour les clients dont le profil est détaillé dans le présent rapport ;
3- Effectuer les déclarations en temps opportun afin de permettre à la CENTIF de faire opposition à l'exécution de l'opération suspectée.

Aux autorités d'enquête de:

1- Initier des enquêtes financières parallèles, en vue d'identifier et de saisir les produits des infractions liées à la cybercriminalité ;
2- Recourir à la coopération internationale à travers les mécanismes existants ;
3- Renforcer la coopération internationale entre les services de renseignement financier et les autorités d'enquête ;
4- Renforcer les capacités des enquêteurs concernant les nouvelles formes de cybercriminalités, surtout celles liées à l'utilisation abusive de la crypto-monnaie ;
5- Renforcer le contrôle dans les cybercafés, qui peuvent parfois servir de plateformes aux activités cybercriminelles ;
6- Sensibiliser davantage sur les méfaits de la cybercriminalité, afin de prévenir victimes potentielles de ce délit.

Aux autorités de poursuites de :

1- Effectuer des enquêtes patrimoniales dans le but de saisir les biens issus de cette criminalité ;
2- Recourir à l'entraide judiciaire internationale ;
3- Renforcer la coopération judiciaire internationale ;
4- Renforcer les capacités des magistrats en matière de cybercriminalité et de l'utilisation abusive de la crypto-monnaie.

Aux populations de:

1- S'informer sur les risques associés à l'utilisation du cyberespace et les mesures de sécurité élémentaires à prendre ;
2- Mettre à jour régulièrement les logiciels antivirus et les pare-feu pour se protéger contre les attaques ;
3- Utiliser des mots de passe forts et uniques pour chaque compte en ligne ;

4- Éviter de partager des informations personnelles sensibles en ligne et de cliquer sur des liens ou des pièces jointes suspectes ;
5- Signaler immédiatement tout incident de cybercriminalité aux autorités compétentes et s'abstenir d'envoyer des fonds à un inconnu.

CONCLUSION :

Pour lutter efficacement contre la cybercriminalité en Côte d'Ivoire, il est essentiel de renforcer les mesures de sensibilisation et d'éducation du public face aux risques liés à l'utilisation du cyberespace. Améliorer la coopération nationale et internationale en matière d'enquêtes et de poursuites.

Il est également nécessaire de renforcer les capacités des autorités compétentes et des assujettis relativement à la lutte contre la cybercriminalité afin de pouvoir détecter, enquêter et collecter des preuves de manière plus efficace et traduire les cybercriminels en justice.