RAPPORT

CHANTIERS DE LA LUTTE CONTRE LA CYBERCRIMINALITE EN CÔTE D'IVOIRE

SEPTEMBRE 2023

Ce rapport a été élaboré par **M. VLADIMIR AMAN,**
Expert cybersécurité et management de la sécurité de l'information,
avec le soutien de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire, pour servir de cadre de réflexion et de propositions dans le cadre de la lutte contre la cybercriminalité en Côte d'Ivoire.

AVANT PROPOS

La Côte d'Ivoire a amorcé un tournant décisif dans son élan de modernisation, avec la volonté clairement affichée au plus haut sommet de l'Etat, de faire du numérique un des leviers principaux de son ambitieux projet d'émergence socio-économique. A un moment où la quatrième révolution est déjà amorcée et menace les Etats à la traine, de manquer une opportunité unique de tirer profit de ce mouvement mondial de transformation structurelle et sociétale, il est de la responsabilité de chacune des forces vives de prendre la pleine mesure de sa responsabilité et jouer sa partition. A l'instar du monde physique, le développement de la société numérique ne devrait pas être l'apanage exclusif de quelques poignées de spécialistes ou dépositaires de pouvoirs publics.

Ce rapport est le fruit de mon engagement à contribuer en qualité d'expert en cybersécurité à mener la réflexion sur les véritables enjeux de la construction d'un cyberespace sain et gage de confiance pour l'ensemble des acteurs de la chaine de valeur.

Analyser et comprendre les enjeux de la sécurité numérique, afin d'actionner les leviers nécessaires à la prise de décisions éclairées et qui servent nos intérêts fondamentaux, c'est bien là toute la motivation qui sous-tend la réalisation de ce travail. Il s'agit évidemment de l'infime contribution d'un praticien au fait de la réalité clinique de la cybercriminalité et des enjeux de développement socio-économiques liés à la sécurité numérique de manière générale, dans un champs exploratoire aussi immense que le cyberespace. En effet, après avoir servi en qualité de référent technique en investigation numérique au sein de la plateforme de lutte contre la cybercriminalité (PLCC), puis comme analyste de cybersécurité, ensuite chef du service cybersécurité et gouvernance de l'internet en charge du développement de la politique nationale de protection des infrastructures critiques et enfin comme Chef du centre de veille et de réponse aux incidents de sécurité informatique de Côte d'Ivoire (CI-CERT), je nourris le rêve de voir une véritable prise de conscience collective des enjeux véritables liés à la cybersécurité.

J'espère que vous trouverez dans ce rapport, des informations, analyses et pistes de réflexions contribuant à alimenter la discussion sur les mécanismes et synergies à mettre en œuvre pour une lutte efficace contre la cybercriminalité en Côte d'Ivoire.

AMAN VLADIMIR
CISSP, CEH, ISO 27032 LCM, ISO 27001 LI

TABLE DES MATIERES

INTRODUCTION

L'essor fulgurant des technologies de l'information et de la communication (TIC) en général et d'Internet en particulier a indéniablement marqué un tournant décisif dans les échanges interhumains. L'Afrique n'a cessé depuis lors de démontrer un intérêt singulier pour les technologies de l'information et de la communication au point d'enregistrer une croissance du nombre d'utilisateurs d'Internet de l'ordre des 13% entre 2000 et 2023, avec plus de 600 millions d'utilisateurs en 2021[1]. Aussi, les implications économiques se font-elles plus vivement ressentir avec l'essor de l'économie mobile. En 2020 par exemple, les technologies et services mobiles ont généré plus de 130 milliards de dollars de valeur économique ajoutée (8 % du PIB) en Afrique subsaharienne. Ce chiffre atteindra 155 milliards de dollars d'ici 2025, avec des recettes et investissements des opérateurs culminants à 56.2 milliards de dollars[2]. Cependant, la fascination, les perspectives d'échanges extraordinaires et de développement économique qu'offre ce moyen de communication nouveau ont vite laissé place à une inquiétude grandissante liée aux usages détournées de cet outil révolutionnaire. En effet, à l'instar de toute innovation majeure, internet a apporté au-delà de ses avantages considérables, son lot de problèmes. Au nombre de ceux-ci, la cybercriminalité s'est imposée depuis de nombreuses années déjà, comme le problème majeur lié à l'usage et à la dépendance grandissante aux TIC.

Quand bien même les priorités et les enjeux restent différents d'un Etat à un autre ou d'un secteur d'activité à un autre, la lutte contre la cybercriminalité demeure un sujet qui réunit les acteurs du monde autour d'un objectif commun. Cette nouvelle forme de délinquance qui rompt fondamentalement avec les caractéristiques de la criminalité classique, reste au centre des inquiétudes des spécialistes de la sécurité informatique, des Etats, des entreprises et même des simples usagers de ces technologies. La multiplication des initiatives concertées tant au niveau international (convention de Budapest, Forum Internationaux sur la cybercriminalité, etc.), que régional en est une des illustrations les plus expressives.

Même si son apparition reste relativement très tardive en Afrique en général, l'essor d'internet sur le continent y a entrainé une explosion exponentielle de cette nouvelle forme de criminalité. Entre infractions classiques (escroquerie, diffamation, etc.) facilitées par l'usage des TIC et infractions nouvelles spécifiques aux TIC, l'Afrique en général et la région occidentale du continent en particulier est enclin à une montée en puissance de la cybercriminalité. Les arnaques en ligne réalisées par l'envoi massif d'e-mails frauduleux et plus connues sous l'appellation de « scam » ou « arnaque à la Nigériane », illustrent très clairement la forte activité cybercriminelle qui prévaut dans cette partie du continent. L'explosion fulgurante de la cybercriminalité dans cette région de l'Afrique et les enjeux y associés, ont poussé les Etats et autres acteurs majeurs de l'industrie du numérique à se pencher avec plus d'intérêt sur la problématique.

[1] https://www.internetworldstats.com/stats.htm
[2] https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_French_Web_Singles.pdf

Dans le cadre juridique Ivoirien, elle recouvre trois grandes catégories d'infractions :

- les infractions spécifiques aux TIC (chapitre 3):
- Les infractions favorisées par les réseaux de communications électroniques (chapitres 4&5):
- Les infractions pénales classiques adaptées aux TIC (chapitre 7):

En Côte d'Ivoire, la dynamique de lutte contre la cybercriminalité s'est traduite par la mise en œuvre de nombreuses mesures d'ordre stratégique, organisationnel, institutionnel et juridique. En outre, la mise en place progressive de mécanismes de coopération avec l'ensemble des acteurs internationaux sont entre autres les quelques mesures prises pour tenter de contrôler ce phénomène criminel transfrontalier. En effet, Internet par sa structure et son modèle de fonctionnement a fait tomber les conceptions classiques de frontières physiques et de territoire entre les pays. La coopération et la concertation entre les différentes forces vives de toutes les nations est une quasi-obligation, si l'on veut trouver des réponses cohérentes aux problèmes que pose la cybercriminalité.

Cependant, bien que des initiatives et efforts aient été engagés çà et là pour juguler le phénomène, force est de constater que l'ensemble des mesures prises semblent ne pas tenir compte des véritables enjeux de la lutte contre le phénomène. En effet, la cybercriminalité telle que perçue par l'imaginaire collectif en Côte d'Ivoire, se résumerait essentiellement aux actes de cyberescroquerie, offrant par conséquent une évaluation restrictive de la menace et des conséquences du phénomène. L'impact véritable de la cybercriminalité demeure inconnu et ce manque d'information conduit à des politiques mal informées et à une évaluation peu cohérente de la problématique.

Alors que le cyberespace est désormais considéré comme un nouvel espace au même titre que les espaces terrestre, maritime et aérien ; la question de sa protection et de sa sécurisation entre naturellement dans le champ des compétences régaliennes de l'Etat. Cependant, il faut avoir la lucidité de reconnaitre que les Etats en général et ceux de l'Afrique de l'Ouest en particulier, n'ont ni le loisir, ni les capacités opérationnelles d'assurer isolément cette mission. Elle interroge toute la communauté des acteurs du numérique sur la nécessité de définir de nouveaux paradigmes et doctrine en matière de sécurisation du cyberespace. Ce rapport propose d'analyser les origines primaires de l'expansion du phénomène en Côte d'Ivoire, pour ensuite poser les bases d'une réflexion prospective et analytique sur les mécanismes et stratégies existants et ceux à mettre en œuvre, afin de garantir aux citoyens et aux entreprises un cyberespace sûr et porteur de développement économique et social soutenu par le numérique.

1.

AUX ORIGINES DE LA CYBERCRIMINALITÉ EN CÔTE D'IVOIRE

1.1. De la pénétration d'internet en Côte d'Ivoire

Sur le continent Africain, seulement deux (02) pays à savoir l'Afrique du Sud et l'Egypte avaient accès aux ressources d'Internet jusqu'en 1994. L' avènement d'internet dans la majorité des pays d'Afrique Subsaharienne a été précédé d'une période de portage, qui correspond à une sorte de période de « tutelle », au cours de laquelle les pays du Nord assuraient la disponibilité et la mise en service de l'infrastructure nécessaire aux échanges via Internet. Pourtant, les premiers signes d'activité par internet remontent à 1988, quand des opérateurs africains de télécommunications ont installé des réseaux X25[3] reliant le nœud national des pays concernés (Sénégal, Mali, Burkina Faso, Côte d'Ivoire, Guinée, Niger, Togo) au centre de coordination et d'appui technique du RIO[4], situé à Montpellier, via le nœud de transit international également situé en France pour répondre aux besoins des entreprises et des industries (transfert de fichiers et téléinformatique).

Plusieurs autres réseaux étaient déjà établis et fonctionnels dans la partie occidentale de l'Afrique, notamment SYTRANSPAC[5] (1989), EARN[6] (1988). Par ailleurs, Abidjan fut déclarée à l'occasion des 4e journées africaines d'informatique en 1988, premier nœud africain du réseau télématique EARN localisé au CIRCI (Centre ivoirien de recherche et de communication internationales). Il utilisait le protocole NJE (Network job entry) avec messagerie, conférences électroniques, téléconsultations de banques de données (Desbois et Vidal, 1989), centre de calculs, etc. L'accès à EARN permettait de recevoir et d'envoyer des messages à d'autres personnes qui étaient dans des réseaux différents comme Internet, Hepnet (hautes énergies), Peacenet (ONG œuvrant pour la paix), Bionet (biologie moléculaire), Fidonet (ordinateurs compatibles PUDOS), Usenet (pour les conférences), etc.
A l'instar de la majorité des pays d'Afrique Subsaharienne, les services internet ont précédé l'implémentation de l'Internet. C'est-à-dire que ces services étaient déjà utilisés dans le pays, bien avant que l'architecture et l'infrastructure nationale ne soit disponible. Selon une étude publiée par la Maison des Sciences de l'Homme de l'Aquitaine (MSHA), on devrait considérer qu'un pays dispose d'Internet des lors que trois conditions sont satisfaites, à savoir :

- Le domaine national a fait l'objet d'une déclaration d'ouverture auprès de l'INTERNIC ;
- Un organisme national gère la base de noms de domaine ;
- Un serveur de noms de domaine est installé sur le territoire national.

Sur la base des critères précités, on peut estimer que l'implémentation d'Internet en Côte d'Ivoire remonte à l'année 1995. En effet, le domaine **« .ci »** a été ouvert auprès de

[3] Réseau de transmission de données par paquet. X25 est la référence de la norme IS0 (International Standard Organisation) qui définit ces réseaux.[PUJSO] TRANSPAC est un réseau public X25.
4 Réseau Intertropical d'Ordinateurs
[5] SYTRANSPAC :Systèmes de transmissions par paquets. c'est le réseau public ivoirien de transmission de données.
[6] EARN: Europeean Academic and Research Network

l'INTERNIC en 1995 par l'ORSTOM[7]. De plus, la base de noms de domaine était déployée au plan local et la gestion du support technique assurée par l'Institut National Polytechnique Houphouët Boigny (INPHB), quoique les serveurs principaux étaient toujours hébergés à Montpellier (France).

Par ailleurs, le « Telecommunications Act », législation américaine visant à accroître la concurrence sur le marché téléphonique pour les services locaux et interurbains a été adopté par le congrès en janvier 1996 et promulgué par le Président Bill Clinton en février 1996. En effet, cette loi Américaine a été conçue en partie pour soutenir l'innovation technologique et des services en permettant aux sociétés américaines de pénétrer de nouveaux marchés, notamment les services de téléphonie longue distance et d'information. En plus de créer une forte concurrence au sein des zones d'échange local qui étaient des monopoles depuis 1934 aux Etats-Unis, cette loi a entrainé l'ouverture à un marché estimé à plus de 200 milliards de dollars. Il s'agissait sans aucun doute de la première réforme majeure depuis la loi originale sur les télécommunications de 1934, qui a ensuite été vigoureusement portée par le lobbying et l'influence du gouvernement Américain. Pour permettre aux entreprises Américaines d'attaquer les marchés prometteurs notamment en Afrique, le gouvernement des Etats Unis à suscité des reformes du secteur des télécommunications dans de nombreux Etats Africains avec comme contrepartie un appui au déploiement de l'infrastructure internet à travers l'initiative Leland. En effet, par suite de la libéralisation du secteur des télécommunications Internet est disponible en Côte d'Ivoire depuis 1996 grâce à l'aide de l'initiative Leland de l'United States Agency for International Developpement (USAID), qui a apporté une assistance technique et matérielle en vue de l'installation d'un nœud national d'accès à CI-Telecom. L'entreprise privée Africa Online devenait ainsi, le premier fournisseur d'accès pour les entreprises et les particuliers, en offrant les services de courrier électronique en 1996. Ensuite, l'accès à Internet a été ouvert au public en Juillet 1996 et à l'initiative du SYFED et du Centre culturel français a été créé le premier cybercafé au cours de la même année.

Cependant, l'accès du grand public à internet, reste très marginal en raison notamment des coûts exorbitants. Pour une installation informatique permettant l'accès à Internet, les coûts à Abidjan étaient de l'ordre 700 000 à 1 000 000 FCFA pour un ordinateur, et 300 000 FCFA pour un modem en 1999. Par exemple, l'abonnement à Africa Online (USA) qui a établi un serveur à Abidjan en 1997, était de 60 à 75 000 FCFA par mois.

La mise en application de la déclaration[8] des pays membres de l'Organisation mondiale du commerce (OMC, Singapour, déc. 1996) relative à la diminution progressive des droits de douane sur le matériel technique et informatique de la communication et de l'information et leur suppression en l'an 2000, allait avoir un impact considérable sur l'accessibilité à internet en Côte d'Ivoire. Les prix baisseront jusqu'à 30 000 FCFA par mois en 2000, mais resteront tout de même largement inaccessible au grand public, dans un contexte économique où le salaire minimum garanti était de 37 000 FCFA.

[7] ORSTOM : Office de la Recherche Scientifique et technique Outre-Mer, anciennement Office de la recherche scientifique coloniale
[8] https://www.wto.org/french/thewto_f/minist_f/min96_f/wtodec_f.htm

1.2. Les prémices d'une cybercriminalité locale naissante

Alors que l'accès au service internet était limité à quelques privilégiés en Côte d'Ivoire, le Sénateur Edward J. Markey et d'autres sénateurs introduisaient en Mai 1998 au congrès Américain, un projet de loi N° H.R. 3916 et intitulé : « Nigerian Advance Fee Fraud Prevention Act of 1998 ». Le descriptif du projet de loi indiquait : « *Nigerian Advance Fee Fraud Prevention Act of 1998 - Exprime le sentiment du Congrès que les États-Unis devraient : (1) travailler avec la communauté internationale pour assurer la poursuite des arnaqueurs nigérians impliqués dans le système de fraude par paiement anticipé (également connu sous le nom de fraude 4-1-9); et (2) prendre toutes les mesures nécessaires pour éduquer le public sur le système et prévenir de futurs incidents. Charge les secrétaires d'État et du Trésor de faire rapport conjointement au Congrès sur les efforts déployés pour informer les citoyens américains des fraudes 4-1-9 et des mesures prises pour les éliminer*».

Le projet de loi visait en effet, à doter le gouvernement Américain d'outils juridiques et institutionnels, afin de prévenir et lutter contre la fraude à la commission d'origine nigériane ou scam 419 (advance fee fraud), dont étaient très largement victimes les citoyens Américains. En effet, dans l'exposé listant les justificatifs de ce projet de loi, l'on note que quinze hommes d'affaires dont deux citoyens Américains avaient été assassinés après avoir effectué des voyages au Nigeria subséquemment à des scam 419. En outre, le préjudice financier causé par le scam 419 excédait les 100 000 000 de dollars US et les sommes tirées de cette activité illicite servaient à financer d'autres activités criminelles incluant le trafic de drogue et les crimes violents. Sous les pressions diverses de la communauté internationale et avec le soutien matériel et technique des Etats-Unis d'Amérique, le gouvernement Nigérian a initié ses premières réponses concrètes contre la scam 419. Les premières réponses du gouvernement Nigérian au phénomène de la cyberescroquerie sont apparues au cours de l'année 2002, avec la création et la mise en ligne du site web « **www.nigerianfraudwatch.com** » . La mise en ligne de ce site web marque la première réaction officielle du gouvernement proportionnée à la menace que représentait la cybercriminalité pour son image et partant son économie. Il s'agissait également de la première réaction face à la criminalité usant d'outils de TIC, au niveau sous-régional. De nombreuses autres actions concertées entre le gouvernement Nigérian et celui des Etats-Unis ont été menées, dont l'implémentation à Lagos d'une représentation des services secrets Américains pour lutter contre la cybercriminalité. Ensuite, des organes institutionnels opérationnels pour lutter contre le cybercrime ont vu le jour, faisant ainsi du Nigéria un terrain de jeu de moins en moins favorable pour les scammers. L'on estime que la mise en place d'une stratégie de lutte fortement répressive sur le plan national a poussé les cyberescrocs à quitter le territoire Nigérian pour trouver refuge dans des zones plus propices à l'exercice de leur activité criminelle.

Dans le même temps en Côte d'Ivoire, entre 1998 et 2001, le taux de pénétration à internet est passé de 1,70% à 6,07% soit environ plus de 12 000 abonnés, servis par (4) quatre fournisseurs d'accès internet. Le gouvernement ivoirien a poursuivi ces actions en faveur de la vulgarisation d'internet au plan national à travers la création du ministère des nouvelles technologies avec un accent particulier sur le développement de cyber centres communautaires, pour faciliter l'accès à internet au grand public. En effet, à l'occasion des Journées des Télécommunications, de l'Informatique et de l'Internet, M. Lia Bi Douayoua, ministre ivoirien de la Communication et des Nouvelles technologies de l'information confiait : « *Nous allons installer des télécentres dans les villages et au niveau du matériel informatique, nous avons un groupe de travail qui réfléchit aux moyens à mettre en œuvre pour que les prix soient plus intéressants. Il faut en particulier des aménagements fiscaux* ».

L'année 2002 marquera une dégradation plus profonde du climat socio-politique avec une tentative de coup d'État armé, qui se soldera par une scission définitive du territoire national en deux parties. Le pouvoir de contrôle et d'application des prérogatives régaliennes de l'Etat s'en verra considérablement réduit, dans un contexte socio-économique qui ne cessa de se précariser. En Avril 2008, des émeutes contre la vie chère éclatent à Abidjan, signe des conditions de vie particulièrement difficiles pour les populations, poussant le gouvernement à céder face à la pression populaire en décrétant un allègement des taxes pesant sur les denrées de base. Pendant ce temps, le taux de pénétration d'internet atteignait les 51,82% en 2008, avec un cadre légal et réglementaire qui n'avait pas évolué pour prendre en compte les récents développements technologiques, notamment l'explosion d'internet. Par ailleurs, selon les statistiques publiées par l'agence de régulation des télécommunications (ATC), 50% des utilisateurs accédaient à internet via le mobile et seulement 1,71 via l'internet fixe.

En outre, dans le contexte de crise économique et politique dans lequel était plongé la Côte d'Ivoire, une subculture urbaine naissait dans la ville d'Abidjan : le couper-décaler. Alimentée par un genre musical du même nom, cette subculture portait les gênes d'un modèle axiologique et normatif alternatif, face à un état affaibli et une culture dominante désorientée. En effet, face aux difficultés de la vie quotidienne rythmée par des discours souverainistes d'un côté et interventionnistes de l'autre, le couper-décaler en tant que subculture urbaine proposait des objectifs et moyens d'action autres que ceux offerts par la culture dominante. Comme le « zouglou » qui était né quelques années plus tôt (1990) dans des conditions quasi-similaires, la subculture « couper-décaler » disposait de ses propres images, normes comportementales, langage, genre musical, mode de pensées, etc. Un des pionniers de ce mouvement, surnommé « DOUK SAGA », sortait en 2003 le premier single du genre musical couper-décaler, intitulé « SAGACITÉ ». Entre autres concepts créés dans la même mouvance, *le travaillement* qui consiste à jeter des coupures de billets de banque sur une personne ou un artiste pour l'encourager ou le rétribuer, visait également à faire l'apologie de la personne qui « *travaille* ». Douk Saga promeut un style de vie hédoniste et affiche son aisance matérielle en portant notamment des vêtements et des bijoux de marque et de grande valeur. Il fait partie des boucantiers,

comme on appelle dans le jargon du couper-décaler les personnes qui aiment s'amuser en boîte de nuit et faire parler d'eux par leur style de vie ostentatoire.
Dans un contexte d'anomie généralisée et face à un affaiblissement de l'identité de classe, le couper-décaler est devenu une nouvelle forme d'identification collective, faisant foisonner des solutions imaginaires aux problèmes structurels de la population, dont notamment le fameux concept de la dette coloniale.

En outre, l'immigration est un facteur caractéristique et un rouage essentiel de l'économie ivoirienne, en particulier depuis que le pays a progressivement adopté une politique relativement ouverte dans les années 60. Depuis son indépendance en 1960, la politique d'immigration de la Côte d'Ivoire est relativement ouverte et a généré des niveaux d'immigration élevés dans le pays. La législation du travail et de la sécurité sociale sont ainsi inclusives en Côte d'Ivoire et l'accès à l'école publique est ouvert à tous sans condition de nationalité ni de statut migratoire. En effet, avec l'ordonnance n°2007- 604 du 8 novembre 2007 portant suppression de la carte de séjour, les étrangers originaires de la CEDEAO ne sont plus soumis à la détention de la carte de séjour. Désormais, le permis de libre circulation sert de titre de séjour aux ressortissants de la CEDEAO lorsque le séjour est inférieur ou égal à trois mois. La carte de résident est utilisée pour les séjours supérieurs à trois mois. Paradoxalement, dans le contexte de crise politico-militaire le gouvernement a adopté plusieurs mesures favorisant encore plus l'immigration des populations des pays voisins, créant un afflux massif de ressortissants étrangers.

1.3. Implantation et expansion du phénomène

La sous-culture cybercriminelle a été importée dans l'espace ivoirien principalement à partir de l'année 2002 dans le contexte de guerre politico-militaire, par des populations immigrées sous-régionales anglophones, composées en majorité de Nigérians et de Ghanéens. En effet, le phénomène criminel était déjà très largement développé au Nigeria, qui avaient d'ores et déjà mis en place des mécanismes répressifs et organisé la lutte contre la cybercriminalité. Face à la relative traque qui s'y organisait, les cybercriminels ont progressivement migré vers le Ghana, eu égard à la proximité culturelle et linguistique. Selon le rapport du Internet Crime Complaint Center (IC3)[9] de 2008, deux pays africains de la sous-région étaient comptés parmi le top 10 des pays avec le plus de cyberdélinquants, notamment le Nigéria (3e) et le Ghana (7e).
Avec un environnement des TIC en plein essor illustré par la prolifération des cybercafés, l'augmentation du nombre d'usagers et un contexte de crise politico-militaire qui avait plongé le pays dans une crise d'anomie généralisée, la Côte d'Ivoire présentait les prédispositions idéales pour « accueillir » cette nouvelle forme de criminalité. On assistait alors à un exode progressif d'un flux de porteurs de la sous-culture délinquante de la

[9] https://www.ic3.gov/Media/PDF/AnnualReport/2008_IC3Report.pdf

cyberescroquerie venus du Nigéria et du Ghana à partir de l'année 2002. Cet exode allait s'intensifier au cours des années suivantes avec la dégradation du climat socio-politique et l'affaiblissement des mécanismes de contrôle des frontières et de lutte contre la criminalité.

La sous-culture délinquante créée par ces flux de « yahoo-boys[10] » du Nigeria & « sakawa-boys[11] » du ghana s'est progressivement encrée dans le paysage sociologique ivoirien de 2002 jusqu'à 2006. L'interpénétration entre ces sous-cultures criminelles et une bonne frange des populations locales, des jeunes en majorité, s'est opérée quand les cybercriminels venus du Nigeria ont entrepris à cause du durcissement des cibles anglophones, de s'attaquer à un « nouveau marché ». En effet, les mesures de sensibilisation et prévention contre le scam 419 mises en place par le gouvernement Nigérian, avec l'appui des Etats Unis d'Amérique, ont eu pour effet de rendre les populations anglophones (des pays majoritairement touchés par le phénomène) de moins en moins vulnérables à ces formes nouvelles d'arnaque. Rendant ainsi le terrain de jeu, moins propice à l'exercice de l'activité cybercriminelle.

On peut considérer que cet état de fait est, en sus des raisons évoquées plus haut, l'un des motifs qui ont poussé les cybercriminels Nigérians et Ghanéens, à *investir la Côte d'Ivoire*. Cependant la barrière linguistique allait constituer un véritable challenge pour « attaquer le marché francophone ». En effet, l'échafaudage des stratagèmes constitutifs des arnaques nécessitait, pour être crédible et avoir des chances de prendre des victimes au piège, une relative maitrise de la langue française. La majeur partie des premières cyberescroqueries enregistrées à cette période et visant des francophones était facilement reconnaissable à son contenu élaboré de manière hasardeuse et dans un maladroit mélange de français et d'anglais.

Une relation de dépendance entre les deux groupes sociologiques prenait ainsi progressivement forme. Les cybercriminels anglophones, Nigérians pour la plupart, s'attachaient ainsi les services de jeunes Ivoiriens ayant une maitrise basique de la langue française, comme interprètes ; afin de réaliser leurs escroqueries. On peut en conclure que par acculturation, des jeunes Ivoiriens ont adhéré aux modes de vie délinquantiels structurant les sous-cultures de yahoo-boys. En effet, l'acculturation désigne les phénomènes qui se produisent lorsque des groupes d'individus viennent en contact continu, et les changements qui s'en suivent dans les modèles culturels d'un ou des deux groupes.

Le développement de la cyberescroquerie en Côte d'Ivoire découle donc en grande partie de l'apprentissage progressif et continu des rouages du « Scam 419 » par des acteurs locaux auprès de pairs plus chevronnés.

Philippe Breton et Serges Proulx évoquent le concept « d'appropriation », pour définir des situations particulières d'apprentissage et d'adhésion totale à un mode de vie. Selon les auteurs, pour parler d'appropriation, trois conditions sociales doivent être réunies.

10 Terme désignant les cyberescrocs au Nigéria
11 Terme désignant les cyberescrocs au Ghana

Tout d'abord, l'usager doit démontrer un minimum de maitrise technique et cognitive de l'objet technique. Ensuite, la maitrise devra s'intégrer de manière significative et créatrice aux pratiques quotidiennes de l'usage. Enfin, l'appropriation ouvre des possibilités de détournements, de réinvention ou même de participation directe des usagers à la conception des innovations .

Sur la maitrise technique et cognitive de l'objet technique, les actes préparatoires techniques d'un scam sont relativement très peu complexes, partant de l'usage d'une boite e-mail à la rédaction et l'envoi d'un simple courriel. Le cœur de l'infraction restant le montage du subterfuge et la manipulation psychologique. En outre, il s'agissait essentiellement de réaliser des scam en français, pour des acteurs disposant de bases minimum. A ce titre, on pouvait noter à cette époque le piètre niveau de langue et d'écriture des courriels de cyberescroquerie. Enfin, la réinvention des techniques et codes transmis par les pairs anglophones a conduit à la naissance du « brouteur », sorte de version améliorée et contextualisée du Yahoo-boy ou du sakawa-boy.

L'appropriation de cette sous-culture délinquante, dans le contexte de crise sociopolitique, économique et sécuritaire précaire dans lequel était plongé le pays a favorisé l'éclosion d'une nouvelle catégorie de criminels. Rompus aux arcanes des escroqueries en ligne et certes façonnés dans le moule des Yahoo-boys et autres sakawa-boys, les « brouteurs » affichant des spécificités totalement locales et adaptées au contexte sociologique Ivoirien, allaient devenir à partir de 2007, les nouveaux « maitres du jeu » dans le cyberespace francophone.

Même si le terme « brouteur » a été vulgarisé et médiatisé avec l'essor des cyberescrocs ivoiriens, il était déjà largement utilisé dans les milieux de la criminalité économique et plus spécifiquement dans le secteur bancaire pour désigner les escrocs dont la spécialité était la production ou l'usage de faux en écriture privée de commerce ou de banque et le faux en écriture publique ou authentique (contrefaçon, altération d'écritures, imitation de signatures sur chéquiers, etc.).

En somme, l'analyse des « trajectoires migratoires » de la cybercriminalité en provenance du Nigeria avec les « **Yahoo-boys** », en passant par le Ghana avec les « **sakawa-boys** », ensuite par la Côte d'Ivoire avec les « **brouteurs** », jusqu'à plus récemment au Togo et au Benin avec les « **gaye-men** », indique clairement que les acteurs de cette activité criminelle dynamique prolifèrent :

- dans des espaces géographiques offrant un faible niveau de contrôle, c'est-à-dire très peu structuré sur le plan légal, organisationnel et institutionnel en termes de détection et répression ;
- dans des contextes d'instabilité et/ou de corruption, car les stratagèmes de fraude utilisés trouvent de la crédibilité sur des faits d'actualités (crise militaire, guerre civile, etc.) ;
- dans des espaces géographiques où l'infrastructure réseau et l'accès à internet est relativement développée ;
- dans des zones géographiques où les subcultures urbaines ont un fort impact sur une grande partie de la population.

2.

LES PREMIERES REPONSES DE L'ETAT IVOIRIEN FACE A LA CYBERCRIMINALITE

2.1. Création de la Direction de l'Informatique et des Traces Technologiques

Si depuis 2001, la police nationale a intégré dans son fonctionnement la police scientifique comme service technique de police, tel que stipulé dans la loi N°2001-479 du 09 Août 2001 portant statut des personnels de la police nationale, ce n'est qu'en 2005 qu'une direction de la police scientifique fut mise sur pieds. Cette nouvelle direction se mua deux ans plus tard en une direction générale adjointe chargée de la police scientifique (DGA-CPS) et fut dotée de plus de prérogatives. Dans le courant de l'année 2007, une nouvelle direction chargée d'adresser les nouvelles méthodes de lutte contre la criminalité liée au numérique fut créé par le décret n° 2007- 464 du 08 mai 2007 portant organisation du ministère de l'Intérieur. Cependant, les difficultés d'ordre organisationnel, matériel et logistique ne permettaient pas à cet organe nouvellement créée et très peu outillé en matière de lutte contre la criminalité numérique, de mener des actions sur le terrain, aux lendemains de sa création.
La Direction de l'informatique et des Traces Technologiques est une des branches de la police scientifique avec pour missions principales de conduire les projets technologiques pour la sécurité, réaliser les investigations en matière de cybercriminalité et fournir un appui technologique aux investigations, tel que définies dans le décret n°2011-388 du 16/11/2011 portant organisation du Ministère d'Etat Ministère de l'Intérieur et de la Sécurité.

2.2. Organisation de la 1ère conférence régionale Africaine sur la cybersécurité

Dans la partie francophone de l'Afrique de l'Ouest, c'est donc la Côte d'Ivoire qui faisait office de figure de proue en matière de cybersécurité, sous l'impulsion de l'Union Internationale des Télécommunications (UIT) et de l'Agence des Télécommunications de Côte d'Ivoire (ATCI). En effet, en Mai 2008, le groupe d'étude 17 de l'UIT-T et le deuxième groupe d'experts de haut niveau de l'UIT pour l'élaboration de l'agenda mondial de la cybersécurité, posait les bases de la réaction officielle de l'Etat Ivoirien. En Juin de la même année, l'Agence des Télécommunications de Côte d'Ivoire, organisait le forum national préparatoire de la conférence régionale africaine sur la cybersécurité. Le point d'achèvement de cet élan de réponse aux problèmes que posaient la cybercriminalité s'est matérialisé par l'organisation de la première conférence régionale africaine sur la cybersécurité (AF-CYBERSEC 2008) du 17 au 20 Novembre 2008, avec pour thème « Bâtir un espace numérique de confiance en Afrique ». Dans ce contexte particulier, l'Agende des Télécommunications de Côte d'Ivoire a donc pris les rênes de cet élan de développement de la cybersécurité à travers des initiatives opérationnelles, telles que l'élaboration du plan d'urgence de lutte contre la cybercriminalité et la création centre de réponse aux incidents de sécurité informatique.

2.3. Création du CSIRT[12] national (CI-CERT)

Forte des principales recommandations du forum AF-CYBERSE 08, l'ATCI a mis sur pieds le 19 Juin 2009 par acte de régulation, la première équipe nationale de réponse aux incidents de sécurité informatique dénommée Côte d'Ivoire – Computer Emergency Response Team (CI-CERT). En tant que cellule technique, essentiellement composée d'ingénieurs en informatique et télécommunications disposant des connaissances de bases en investigation numérique et sécurité informatique, le CI-CERT avait pour mission initiale de contribuer à assurer la confiance dans l'utilisation d'Internet par la communauté des Internautes Ivoiriens et appuyer les agences d'application de la loi.

L'Etat Ivoirien disposait sur le plan institutionnel d'une division spécialisée de la police nationale pour la lutte contre la criminalité liée au numérique, mais qui de manière opérationnelle était complétement dépourvue de capacités humaines et techniques en matière d'investigation numérique. De l'autre côté, l'ATCI avait mis en place une équipe de réponse aux incidents de sécurité informatique dotée de moyens humains et techniques nécessaires pour apporter des réponses opérationnelles, notamment en termes d'investigation numérique, de développement d'outils liés à la lutte contre la cybercriminalité. En somme l'Etat Ivoirien disposait de deux acteurs clés, l'un (DITT) disposant de la légitimité légale et de la force publique pour poursuivre les auteurs de cybercrimes, mais dépourvu de capacités opérationnelles en la matière ; l'autre disposant des compétences opérationnelles, mais pas de la légitimité légale nécessaire pour connaitre des affaires judiciaires liées à la lutte contre cybercriminalité.

2.4. Création de la Plateforme de Lutte Contre la Cybercriminalité (PLCC)

Eu égard au contexte d'urgence nationale et pour juguler cette contrainte qui freinait l'action concertée des deux acteurs, les Directeurs Généraux de l'ATCI et de la Police Nationale ont entrepris de mutualiser leurs forces, à travers la signature le 02 Septembre 2011 d'une convention de partenariat portant création de la Plateforme de Lutte Contre la Cybercriminalité (PLCC).

Première du genre sur le plan national, la Plateforme de Lutte Contre la Cybercriminalité a apporté une approche nouvelle dans la lutte contre la criminalité en regroupant au sein d'une même équipe des personnels civils issus du CI-CERT (ATCI) et des fonctionnaires de Police issus de la DITT(Police Nationale). En effet, la plateforme est placée sous l'autorité judiciaire et opérationnelle de la DITT, et mise sous le pilotage administratif de l'ARTCI[13].

En outre, il convient de mentionner que dans le contexte ivoirien, les mesures organisationnelles ont été mises en place en l'absence d'un cadre légal spécifiques à la lutte contre la cybercriminalité. En effet, à cette période les poursuites judiciaires restaient

[12] Computer Security Incident response Team
[13] Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire

limitées et peu efficaces dans la mesure où les infractions nouvellement nées avec le développement de la cybercriminalité n'étaient pas prises en compte dans la code pénal. Dans certains cas, quand bien même les faits étaient clairement démontrés et documentés par les équipes opérationnelles, les autorités judiciaires étaient contraintes à se limiter à des condamnations ou sanctions « ridicules », tant les bases légales étaient peu solides, conformément au principe de légalité pénale.

Les premières réponses de mise à niveau du cadre légal national et de restructuration du secteur des technologies de l'informations et de la communication et des télécommunications sont intervenues en 2012, avec l'adoption de l'ordonnance N°2012-293 du 21 mars relative aux télécommunications et aux technologies de l'information et de la communication. Cette ordonnance a posé les bases du renforcement de l'arsenal légal sur les questions liées à l'émergence du numérique, débouchant au cours de l'année 2013 à l'adoption de la loi N°2013-251 du 19 Juin 2013 relative à la lutte contre la cybercriminalité et d'autres textes de loi connexes.

3.

ETAT DES LIEUX DE LA LUTTE CONTRE LA CYBERCRIMINALITE EN CÔTE D'IVOIRE

3.1. Emergence d'un corpus législatif et règlementaire

Depuis l'ordonnance N°2012-293 du 21 mars relative aux télécommunications et aux technologies de l'information et de la communication, la loi N°2013-251 du 19 Juin 2013 relative à la lutte contre la cybercriminalité et plus récemment la loi N°2021-893 du 21 décembre 2021 modifiant la loi N°2019-574du 26 juin 2019 portant code pénal, la législation Ivoirienne a pleinement pris en compte la problématique de la cybercriminalité. Cet important dispositif législatif est complété par des textes réglementaires notamment le décret[14] n° 2017-193 du 22 mars 2017 portant identification des abonnés des Services de Télécommunications/TIC ouverts au public et des utilisateurs des cybercafés.

La loi N°2013-451 du 19 Juin 2013 est le principal instrument juridique en matière de lutte contre la cybercriminalité en Côte d'Ivoire. Elle intègre tous les instruments juridiques communautaires et internationaux de lutte contre la cybercriminalité, notamment :

- La loi type de la commission des nations unies pour le Droit Commercial International (CNUDCI) sur le commerce électronique (12 juin 1996);
- La Convention de Budapest sur la cybercriminalité (23 Novembre 2001) ;
- L'acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO du (16 Février 2010)
- L'acte additionnel A/SA.2/01/10 portant transactions électroniques dans l'espace de la CEDEAO du (16 Février 2010)
- La Directive relative à la lutte contre la cybercriminalité dans l'espace de la CEDEAO (19 Août 2011) ;
- Le projet de convention de l'Union Africaine sur l'harmonisation des « cyberlégislations » en Afrique (06 Septembre 2012)
- La convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Juin 2014)

Cette loi apporte des innovations en matière de droit pénal substantiel en définissant des infractions nouvelles et fixant les peines associées. Elle prévoit des peines d'emprisonnement allant jusqu'à 10 ans de prison pour des infractions qualifiées « délit », mais réprimées comme des « crimes ». Aux termes de ce texte de loi, les cyber infractions peuvent être divisées en trois catégories:

- **Les infractions spécifiques aux TIC (chapitre 3):**
  - Accès frauduleux dans le système d'information ;
  - Introduction frauduleuse des données dans un système d'information ;
  - Altération, modification ou suppression frauduleuse des données informatiques ;
  - Utilisation frauduleuse d'éléments d'identification d'une personne physique ou morale par le biais d'un système d'information ;
  - Messages électroniques non-sollicités ;
  - Suppression ou détournement des correspondances électroniques.

[14] https://www.artci.ci/images/stories/pdf/decrets/decret_2017_193.pdf

- **Les infractions favorisées par les réseaux de communications électroniques (chapitres 4&5):**
    - Atteintes à la propriété intellectuelle ;
    - Atteintes à la vie privée ;
    - Images ou représentation à caractère de pornographie infantile ;
    - Organisation illicite de jeux d'argent sur les réseaux de communications ; électroniques.
- **L'adaptation des infractions pénales classiques aux TIC (chapitre 7):**
    - Racisme ou xénophobie par le biais d'un système d'informations ;
    - Menaces de mort ou de violences par le biais d'un système d'information ;
    - Trahison au profit d'un pays tiers ;
    - Terrorisme.

De plus, le texte pose ou du moins réaffirme les principes généraux d'investigations judiciaires en matière de cybercriminalité, notamment les principes de territorialité, d'extraterritorialité et d'extradition. Aussi, édite-t-il les règles de procédure pénale spécifiques à la cybercriminalité, en ce qui concerne les mesures de perquisitions, de saisie et de conservation des données électroniques ou informatiques, en matière d'investigation numérique, de preuve électronique et de coopération judiciaire internationale. Même si le texte n'a pas encore été révisé pour tenir compte des nouvelles évolutions en la matière, il couvre tout de même les exigences essentielles des cadres légaux internationaux en matière de cybercriminalité, notamment les conventions de la Malabo et de Budapest.

Au niveau régional et international, la Côte d'Ivoire a ratifié et déposé ses instruments de ratification de la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (convention de Malabo) en 2023. Par ailleurs, la Côte d'Ivoire fait partie des pays signataires et invités à adhérer à la convention de Budapest sur la cybersécurité du conseil de l'Europe. Ce statut indique que l'Etat Ivoirien a déjà mis en œuvre les dispositions de la Convention de Budapest en droit interne, et qu'après une lettre adressée au Secrétaire général du Conseil de l'Europe indiquant son intérêt à adhérer à la Convention de Budapest, les Etats déjà parties à la convention ont marqué leur accord. Les autorités Ivoiriennes devraient conduire les procédures internes de ratification avant de déposer l'instrument d'adhésion près le Conseil de l'Europe.

3.2. Typologie des cybercrimes et acteurs

3.2.1. Types de cybercrimes

Selon les statistiques de la plateforme de lutte contre la cybercriminalité, plus de 90% des cyberinfractions sont constituées d'infractions classiques facilitées par les TIC, à savoir l'escroquerie en ligne (faux héritage, faux sentiments, loterie, assistance covid19, etc.), les fraudes sur porte-monnaie électronique (Ingénierie Sociale, SIM Swap), les chantages à la vidéo (sextorsion) et les faux ordres de virement (imitation de documents numériques). Cependant, une augmentation significative des infractions spécifiques aux TIC à savoir, l'e-mail spoofing, introduction de données frauduleuses dans un système d'information (virus, vers, trojan, etc.), accès frauduleux à tout ou partie un système d'information, les ransomware, etc., a été enregistré par les services de la PLCC et de la Direction de la Police Economique et Financière (DPEF) depuis 2017. En effet, c'est en moyenne trois (3) plaintes pour fraudes ou infractions liées à la cybercriminalité qui ont été déposées par an par les établissements financiers à caractère bancaire auprès de la Direction de la Police Economique et Financière (DPEF) entre 2016 et 2018.
En outre, les acteurs s'engagent relativement tôt dans la cyberdélinquance, autour de 15 ans avec une prévalence de l'ordre des 40% d'élèves et étudiants et 29% de sans emploi, dont 92 % sont des hommes et 10% des femmes.
En ce qui concerne la cartographie des acteurs cybercriminels, nous nous appuyons sur une approche descriptive inspirée de certaines métriques de la méthodologie STIX[15], afin d'établir une photographie actuelle. Sur la base des statistiques collectées par les agences d'application de la loi, quatre critères essentiels peuvent permettre de dresser un aperçu des acteurs cybercriminels en Côte d'Ivoire, notamment la motivation, le niveau de ressources, le niveau d'organisation et le niveau de sophistication.

3.2.2. Motivation des acteurs

Le motif premier est le gain personnel, alimenté par le désir d'améliorer son propre statut financier et social. Les acteurs cybercriminels sont motivés par un désir égoïste de gain personnel provenant de la fraude financière, de l'escroquerie.

3.2.3. Le niveau de ressources

Une grande proportion d'acteurs cybercriminels disposent de ressources limitées d'un individu moyen agissant de manière indépendante. Cependant, bien que la plupart des acteurs agissent à titre individuel, il existe des clubs de pairs au sein desquels les membres interagissent sur une base sociale et bénévole, souvent avec peu d'intérêt personnel sur une cible spécifique. Ces groupes sont plus apparentés à des forums sur

[15] Structured Threat Information Expression

lesquels les acteurs échangent régulièrement des conseils et des procédés, sans entretenir une véritable logique de groupe organisé.
Par ailleurs, l'augmentation des fraudes et cyberattaques contre les établissements financiers à caractère bancaire met en lumière l'émergence progressive de groupes formellement organisés avec un dirigeant, généralement motivé par un objectif spécifique et organisé autour de cet objectif.

3.2.4. Le niveau d'organisation

Le niveau d'organisation reste majoritairement dominé par des acteurs agissant seuls ou en regroupement informel d'acteurs cybercriminels, sans gouvernance établie et liens d'interdépendance ou hiérarchique. Cependant, une montée en charge des initiés incluant toute personne ayant bénéficié d'une confiance interne étendue, tel que des employés réguliers, les prestataires, les consultants et les travailleurs temporaires. Ils jouissent de connaissances étendues des mécanismes et failles de sécurité qui peuvent être exploitées lors de la conduite d'attaques et peuvent prendre un certain nombre d'actions, y compris le vol, la fraude, etc. L'analyse des dernières cyber incidents porte à croire que des groupes persistants, organisés et établis sur le long terme sont en phase de gestation.

3.2.5. Le niveau de sophistication des acteurs

En grande majorité, les acteurs cybercriminels ivoiriens ne justifient d'aucune sophistication, mais plutôt de capacités à effectuer des actes aléatoires de fraude, perturbation ou de destruction en utilisant des outils dont ils ne maitrisent pas vraiment les contours techniques. Ils possèdent des compétences informatiques moyennes.
Cependant, on peut observer une proportion considérable d'acteurs capables d'utiliser au minimum des techniques et des programmes ou des scripts existants et fréquemment connus et faciles à trouver pour rechercher et exploiter les faiblesses des systèmes. Communément appelés script-kiddies, ces acteurs s'appuient sur d'autres pour développer des outils malveillants, des mécanismes de mise en œuvre et une stratégie d'exécution et ne comprennent souvent pas pleinement l'outil qu'ils utilisent ou comment ils fonctionnent.
En revanche, une frange quoique réduite de la population cybercriminelle justifie d'un niveau de sophistication intermédiaire. Ces acteurs peuvent utiliser les cadres d'attaque et les outils existants pour rechercher et exploiter les vulnérabilités des ordinateurs ou des systèmes. Les acteurs de cette catégorie possèdent des compétences informatiques équivalentes à celles d'un professionnel de l'informatique et ont généralement une connaissance pratique des réseaux, des systèmes d'exploitation et peut-être même des techniques défensives, et présentent généralement une certaine sécurité opérationnelle. Ces acteurs comptent sur d'autres pour mettre au point des outils et des mécanismes de mise en œuvre malveillants, mais sont en mesure de planifier leur propre stratégie

d'exécution. Ils sont compétents dans les outils qu'ils utilisent et dans la façon dont ils fonctionnent et peuvent même apporter des modifications minimales au besoin. Ces acteurs sont plus observés au sein des catégories d'initiés, internes et autres groupe structurés ciblant les établissements financiers à caractère bancaire en particulier.

3.3. Développement des capacités opérationnelles de lutte

3.3.1. Au niveau de la police

Depuis la fin des années 2000, la police nationale s'est positionnée comme le principal acteur d'application de la loi en matière de lutte contre la cybercriminalité. Avec son partenariat stratégique avec l'Autorité de Régulation des Télécommunications/TIC dans le cadre de la création de la Plateforme de Lutte contre la cybercriminalité (PLCC), la police nationale a développé des capacités humaines et techniques à la pointe de la technologie. En effet, la Direction de l'informatique et des traces technologiques, bras technologique de la Direction Générale de la Police Nationale, fait partie des trois directions centrales composant la Direction Générale Adjointe chargée de la Police Scientifique (DGACPS). Elle dispose à ce jour de trois unités organisationnelles opérationnelles notamment le centre de fusion et d'analyse de données (CFAD), le poste de commandement central (PCC) et la plateforme de lutte contre la cybercriminalité (PLCC).
Son organisation est structurée autour de ses trois axes d'intervention et comprend :

- **Le centre de fusion et d'analyse de données (CFAD)** : qui œuvre à la valorisation de données numériques pour apporter un soutien aux investigations initiées par tous les services d'application de la loi, notamment les services de police judiciaire, la CENTIF, la gendarmerie, la défense, les services de renseignement, la PLCC, etc.
- **Le poste de commandement central (PCC)** : dont la fonction de soutenir les activités opérationnelles à travers l'usage de technologies numériques notamment le centre d'appel à numéro gratuit 100, le centre de vidéo protection urbaine (vpu) et le centre de traitement des signalements via les réseaux sociaux ;
- **La plateforme de Lutte Contre la Cybercriminalité (PLCC)** : centre opérationnel pour les questions liées à la prévention et aux investigation en matière de cybercriminalité.

Le CFAD représente le centre de capacités de valorisation de données numériques au profit des investigations, avec notamment un laboratoire de criminalistique équipé des dernières technologies numériques. Il reçoit, centralise et analyse les données de toutes les sources et centres de demandes (police, gendarmerie, etc.), afin de produire de l'information actionnable et utile à la conduite des enquêtes judiciaires. A ce jour, le CFAD est en mesure d'analyser la plupart des supports, technologies et protocoles numériques disponibles sur le marché.

Le PCC s'appuie quant à lui sur l'usage des technologies numériques pour soutenir les activités opérationnelles, notamment à travers le réseau national de caméras de vidéosurveillance. Enfin, la PLCC est le fleuron des investigations liées à la constatation, la recherche des preuves et la poursuite des auteurs d'infractions liées à la cybercriminalité.
En outre, les effectifs de la DITT sont constitués d'une centaine d'agents opérationnels intégrant des personnels civils, des fonctionnaires de police et des membres d'autres forces de sécurité. Ils assurent l'animation des opérations de réaction, de veille à travers le poste de commandement de la DITT et de signalement à travers les pages de réseaux sociaux.
Par ailleurs, la Direction de la Police Economique et Financière (DPEF) dispose également d'une cellule d'investigation numérique pour les crimes financiers. Avec plus des 95% des cyber infractions motivés par le gain financier, cette cellule joue également un rôle prépondérant dans la lutte contre la cybercriminalité, bien que son périmètre d'action soit plus étendu.

3.3.2. Au niveau de la justice

Bien qu'il n'existe pas de bureau ou section dotée de prérogatives spécifiques à la cybercriminalité, la justice ivoirienne s'est mise quelque peu à l'heure des évolutions technologiques avec la création d'une juridiction spécialisée pour mener la lutte contre la criminalité économique et financière. En effet, le Pôle Pénal Economie et Financier (PPEF) créé en 2022 par l'adoption de la loi N°2022-193 du 11 mars 2022 est une juridiction de premier degré, autonome spécialisée en matière de délinquance économique et financière. Cette juridiction est chargée de la poursuite, de l'instruction et du jugement des infractions en matière économique et financière. Elle l'exerce sur l'ensemble du territoire national, même si sa compétence est subordonnée à l'existence d'une infraction économique et financière justifiant d'une certaine gravité et complexité particulière. A ce titre, il comprend un siège, un parquet, un greffe et des services administratifs et des magistrats spécialement formés aux dernières techniques de prévention et d'investigations, qui animent cette juridiction. Il existe à ce jour, très peu de magistrats spécialisés dans la cybercriminalité, mais la mise en place de cette juridiction spéciale représente une formidable fenêtre de développement de compétences pour des magistrats spécialisés dans la matière.
Par ailleurs, l'Agence de Gestion et de Recouvrement des Avoirs Criminels chargée d'exécuter les décisions de gel, de saisie et de confiscation des avoirs illicites prononcées dans le cadre de procédures pénales ou administratives a été mise sur pieds depuis 2013. Cette agence composée de neuf (09) hauts cadres de l'Administration judiciaire, financière et économique est compétente pour la gestion et le recouvrement des avoirs criminels gelés, saisis ou confisqués liés à la cybercriminalité.

3.3.3. Au niveau du régulateur des Télécommunications/TIC

L'ARTCI a joué un rôle crucial dans la mise en place des premières capacités opérationnelles de lutte contre la cybercriminalité et plus généralement de cybersécurité sur le plan national, dès le début de l'essor d'internet en côte d'ivoire. Sous sa conduite, l'Etat Ivoirien a entériné par décret N°2020-128, la création du centre de veille et de réponse aux incidents de sécurité informatique dénommé CI-CERT. Cependant, l'équipe a été rendue opérationnelle depuis Juin 2009 et représente depuis lors le premier centre de capacités en matière de veille et réponse au incidents de sécurité informatique. Même si son rayonnement s'est vu quelque peu freiné ces dernières années, le CI-CERT reste la principale porte de coordination de la gestion des incidents, d'alertes sur les vulnérabilités et risques de sécurité impactant les infrastructures critiques et le canal privilégié pour la coopération internationale à travers son adhésion au forum mondial des équipes de réponse aux incidents de sécurité (FIRST) et également au forum africain des équipes de réponse aux incidents de sécurité AFRICACERT.
En outre, le CI-CERT offre des services de base tels que standardisés par la communauté mondiale des CSIRT à toutes ses parties prenantes, mais assiste également les agences d'application de la loi dans le cadre d'instructions judiciaires, pour des cas d'infractions dites « HIGH TECH CRIME » (analyse forensique légale, analyse de logiciels malveillants, ingénierie inversée, etc.). En effet, le CI-CERT est également un acteur majeur de la lutte contre la cybercriminalité et l'investigation numérique légale avec son pool d'agents assermentés et dotés de la qualité d'officiers de police judiciaire, ayant compétence pour conduire tous les actes de police judiciaire dans le cadre de la sécurité liée au numérique.
Par ailleurs, l'ARTCI a mis en place un site web d'information pour la protection des enfants en ligne et une plateforme de signalement de cyber infractions touchant les mineurs, en collaboration avec l'Internet Watch Foundation (IWF). Cette plateforme est accessible à travers le site web https://www.jemeprotegeenligne.ci/ et propose une plateforme de signalement anonyme en quelques clics de cas de pédopornographie et d'abus sexuels sur mineurs en ligne.

3.4. Une meilleure connaissance statistique de la cybercriminalité

Les mesures mise en place depuis 2009 ont permis d'appréhender quoique partiellement, une bonne partie de la réalité de la cybercriminalité en Côte d'Ivoire. En effet, les chiffres présentés ci-après proviennent de la collecte réalisée en s'appuyant sur les rapports d'activités de la PLCC et de la DPEF et du CI-CERT. L'analyse des données statistiques permet en effet, d'évaluer à minima les caractéristiques quantitatives de la cybercriminalité en Côte d'Ivoire.
Entre 2009 et 2022, le préjudice financier direct déclaré à la PLCC et au CI-CERT s'élève à un peu plus 65 milliards FCFA, soit un préjudice avoisinant les 5,5 milliards FCFA en moyenne par année. En outre, sur la même période, 30.029 dossiers de cybercriminalité

ont été traités, représentant un moyenne annuel de d'environ 2304 dossiers de cybercriminalité traités. Par ailleurs, sur la même période considérée, 1.418 suspects ont été interpellés pour des infractions liées à la cybercriminalité, dont 807 ont été déférés devant le parquet. Ce qui représente un ratio d'environ **5% des suspects interpellés** par suite d'une déclaration aux autorités judiciaires et dont **3% seulement aboutissent à un déféremment** des mis en cause devant le parquet.

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	TOTAL
Nombre affaires cybercriminalité	950	1 766	914	1 846	552	564	1 409	2 067	2 408	2 860	4 505	4 886	5 302	6 579	**30 029**
Préjudice financier direct déclaré (millions FCFA)	**N/D**	14 010	N/D	3 385	3 602	5 182	2 535	2 979	3 369	7 414	4 920	6 170	6 320	6 293	**66 179**
Nombre de suspects interpellés	76	76		71	70	93		116	175	89	97	103	181	271	**1 418**
Nombre de suspects déférés	37	68		51	65	65			147	73	92	57	67	85	**807**
Nombre de bulletins de sécurité publiés	84	120	173	462	462	116 440		540	297	297		478	294	950	**120 597**

Tableau 1: Synthèse des statistiques de la lutte contre la cybercriminalité de 2009 à 2022

Cette analyse fourni des clés de lecture objective de la situation réelle en matière de lutte contre la cybercriminalité. En dépit des nombreux efforts consentis, moins de 5% des cas déclarés aboutissent à une présentation devant le parquet. Le nombre de condamnations pour des infractions de cybercriminalité devrait se situer en dessous des 2%, en considérant le niveau relativement moyen de spécialisation des magistrats en matière de compréhension de la cybercriminalité dans ses spécificités techniques. Selon les chiffres de la PLCC, **82%** des cyber infractions sont constituées d'escroqueries et d'abus de confiance, en dépit de l'apparition d'infractions purement technologiques depuis 2017. Aussi, le nombre d'affaires portées devant les service de police n'a cessé de croitre au fil des années, avec des prévisions clairement en faveur d'une hausse à venir .

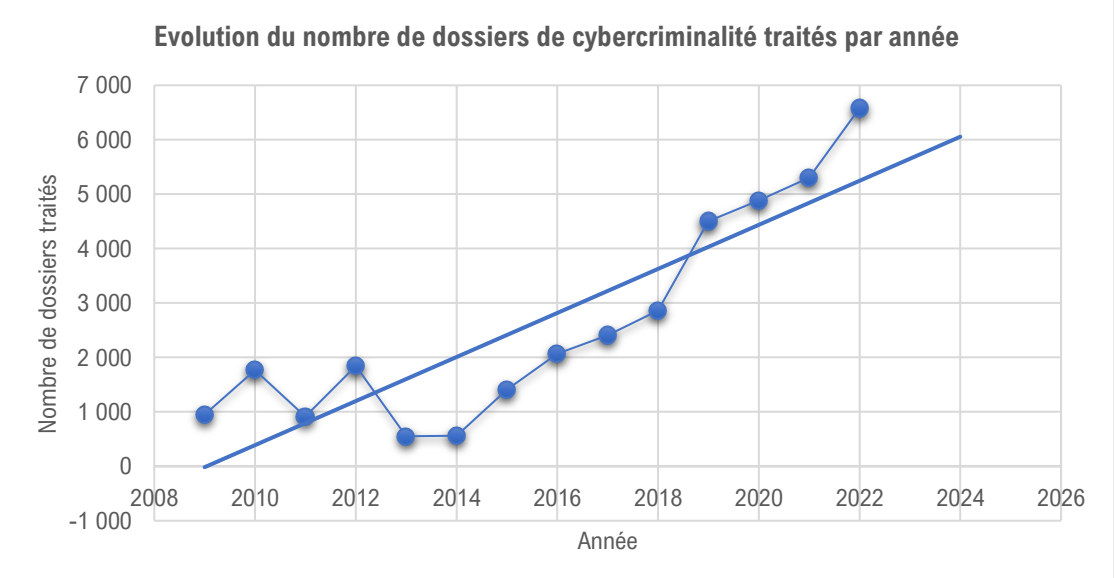

Figure 1: Courbe d'évolution des dossiers de cybercriminalité traités entre 2009 et 2023

En outre, selon les résultats d'une étude[16] réalisée par des chercheurs criminologues ivoiriens, cinquante-quatre (54) établissements bancaires ont déclaré à la DPEF[17] avoir été victimes de cyber infractions, débouchant sur 193 plaintes et un préjudicie financier direct de plus de 27 milliards FCFA. Ces résultats laissent clairement conclure qu'il existe une dispersion et une non centralisation des sources de données policières en la matière. De plus, ces résultats indiquent une hausse progressive d'une cybercriminalité à caractère économique, employant des moyens techniques plus évolués pour un potentiel destructeur plus important. Sur la période d'étude concernée par cette étude, on peut noter que les établissements bancaires sont victimes en moyenne de 3 cyber infractions majeures par an.

Année	Nombre d'établissements bancaires ayant été victime	Nombre de plaintes déposées par des établissements bancaires	Préjudice financier (FCFA)
2016	13	50	2 860 649 950
2017	18	68	9 002 142 915
2018	23	75	15 288 977 009

Tableau 2: Statistiques des cyberattaques bancaires traités par la DPEF de 2016-2018

Par ailleurs, selon des données statistiques policières collectées auprès de la DPEF, depuis 2020, le préjudice financier direct des cyber infractions contre les établissement financier et bancaires, s'élève à plus de cinq (5) milliards de FCFA, répartis comme suit :

Année	Préjudice
2020	2 013 592 279
2021	1 000 000 000
2022	192 060 174
2023*	1 849 332 901

En somme, la lecture des données statistiques met en lumière une relative difficulté à mettre en cohérence et centraliser les données collectées liées à des cyber infractions. A cette difficulté s'ajoute l'imprécision dans l'évaluation du préjudice financier direct subi par les victimes au moment où les infractions sont portées à la connaissances des autorités policières. Il est clair que les mécanismes de collecte de signalement permettent à minima de faire un état du préjudice des cyberincidents, mais il apparait qu'une grande part de l'impact financier réel des cyberattaques échappe totalement aux acteurs (services de police, victimes, magistrats).

[16] CYBERCRIMINALITE ET BANQUES EN COTE D'IVOIRE Par AKADJE Ahiouré Mathieu, AZI Josselin Wilfred, AZI Eléonore Epouse Diabaté, P.116
[17] Direction de la Police Economique et Financière

3.5. Etat de la recherche, des connaissances scientifiques et techniques sur la cybercriminalité

Au niveau de la recherche scientifique, de plus en plus d'articles scientifiques et travaux de recherches sont entrepris par des chercheurs issus de domaines de spécialités divers. En effet, ces derniers années ont enregistré un intérêt croissant pour des travaux scientifiques ou techniques sur la lutte contre la cybercriminalité, notamment au niveau de l'Institut National de Formation judiciaire et de l'UFR de Criminologie de l'Université Félix Houphouët Boigny. Cependant, ces productions restent quelques peu confinées strictement au monde académique et apparaissent déconnectées du monde des praticiens. En tout état de cause, il est quasi impossible de mesurer l'impact des travaux de recherche scientifique sur la cybercriminalité, car très peu de passerelles sont établies entre ces différents mondes pour permettre de tirer profit des avancées techniques et scientifiques issus des différents mondes de production de connaissances.
Au niveau de la recherche et développement (R&D), il n'existe quasiment aucune initiative nationale tant publique que privée spécifique à la lutte contre la cybercriminalité. L'absence de communication entre les monde de la recherche et clinique ne favorise par une définition des objectifs et besoins de recherche et développement appliqués à la cybersécurité de manière générale.

3.6. Prédictions d'évolution de la cybercriminalité

Si la cybercriminalité légale situe actuellement à plus de 80% le nombre de cyber escroqueries classiques, cette tendance devrait très vite basculer dans les quatre voire cinq prochaines années. Les cyber escroqueries de type romance scam, arnaque au président et autres formes de cyber arnaques et manipulations psychologiques devraient rester relativement présentes dans le panorama des cybercrimes, avec l'émergence de technologies facilitant l'échafaudage des subterfuges. On devrait raisonnablement s'attendre à l'explosion de l'usage de l'intelligence artificielle dans les cyberescroqueries, avec l'exploitation des capacités de modèles d'IA générative pour créer des « vrai faux » contenus. Les prémices de ces usages détournés des IA pour réaliser des cyberescroqueries sont déjà perceptibles avec les modèles capables de traduire instantanément les paroles d'une vidéo dans différents langues, générer des personnages fictifs plus que réalistes à partir de photos, etc.
Cependant, une montée progressive et déjà perceptible de cybercrimes impliquants des moyens techniques plus évolués devraient s'installer en tête des menaces liées à la cybercriminalité. En effet, avec trente (30) établissements de crédits dont vingt-huit (28) banques et deux (2) établissements financiers, la Côte d'Ivoire représente plus de 33% de part de marché du secteur bancaire et financier de l'Union Monétaire Ouest Africaine

(UMOA) selon le rapport d'activités[18] 2021 de la commission bancaire de la BCEAO. Elle représente le plus gros marché de l'UMOA avec plus de 5,4 millions de comptes bancaires et un bilan estimé à plus de 18.000 milliards en 2021. Le secteur bancaire et financier Ivoirien affiche une dynamisme remarquable qui attise la convoitise des investisseurs et des cybercriminels également. Cependant, ce fort dynamisme contraste avec la relative porosité des systèmes de défense et mécanismes de sécurité déployés dans les établissements bancaires et financiers. Dans une étude intitulée « OPERA1ER Playing god without permission[19] », le groupe privé de lutte contre la cybercriminalité révélait qu'entre 2018 et 2021, sur 30 cyberattaques attribuées au groupe cybercriminel OPERA1ER dans le monde, douze (12) avaient été réalisées en Côte d'Ivoire. Cette étude met en lumière le fait que la Côte d'Ivoire est un terrain de jeu plus que favorable, tout d'abord en raison du grand dynamisme de son secteur bancaire et du faible niveau de préparation et de sécurisation global des systèmes d'informations critiques des établissements bancaires.

On devrait voir se ruer vers la Côte d'Ivoire dans un premier temps, des syndicats du cybercrime opérant depuis l'extérieur des frontières géographiques du pays, avec la participation de relais locaux, coordonnateurs pour l'orchestration des fraudes, des administrateurs et employés des établissements bancaires pour leur facilitation et des mules recrutés comme tireurs. Le secteur bancaire sera indéniablement le théâtre de cette mutation brutale de la cybercriminalité en Côte d'Ivoire, avant de s'étendre à d'autres secteurs comme les télécommunications et l'énergie. Cette tendance est appuyée par les récentes opérations d'envergure réalisées par Interpol et qui ont conduit au démentiellement partiel de nombreux syndicats du cybercrime organisé en Afrique de l'Ouest, notamment Silver Terrier, Opera1er, etc. Même si Interpol[20] affirme avoir interpellé un suspecté membre influent du groupe Opera1er à Abidjan lors d'une opération conjointe avec la DITT, la grande majorité des acteurs de ces groupes cybercriminels organisés sont localisés au Nigeria.

Il faudra s'attendre dans une seconde phase à ce que le panorama des menaces bascule des simples arnaques, vers des campagnes de spear phishing, mettant en œuvre des logiciels malveillants de type RAT (Remote Administration Tool ou outil de contrôle à distance) clés en main, comme moyen d'accès initial aux systèmes. Dans cette phase, l'on pourrait voir se multiplier les attaques de type compromission d'emails professionnels (BEC[21]) basée sur des outils développés par des acteurs plus chevronnés situés hors des frontières géographiques du pays et débouchant sur l'exploitation de vulnérabilités des systèmes d'information.

La troisième phase de cette mutation de la cybercriminalité devrait, à l'instar de la première appropriation du phénomène des scams 419 du début des années 2006, marquer une explosion des cyberattaques plus sophistiquées et persistantes. En effet, avec la multiplication des efforts de vulgarisation en termes de formation à la

[18] https://www.bceao.int/sites/default/files/2022-08/Rapport%20annuel%202021%20de%20la%20Commission%20Bancaire.pdf
[19] https://go.group-ib.com/report-opera1er?_gl=1*j27qnq*_ga*MTcxNjY4MTg5LjE2OTIxOTExOTA.*_ga_QMES53K3Y2*MTY5MjE5MTE4OS4xLjAuMTY5MjE5MTE4OS42MC4wLjA.
[20] https://www.interpol.int/News-and-Events/News/2023/Suspected-key-figure-of-notorious-cybercrime-group-arrested-in-joint-operation
[21] Business email compromise ou compromission d'e-mails professionnels (BEC)

cybersécurité, au codage informatique, etc. ; une promotion de jeunes geeks formés et rompus aux techniques les plus avancées de développement de logiciels malveillants et d'exploitation des failles des systèmes informatique verra le jour. Il est à craindre de ce fait, une appropriation par la nouvelle génération de passionnés de hacking de cette sous-culture cybercriminelle emmenée par le contact et l'interpénétration avec les groupes cybercriminels organisés. Cette projection dans le futur de la cybercriminalité ivoirienne laisse entrevoir un développement fulgurant de places de marchés illicites dans le « black cybermarket » qui se positionnera incontestablement comme la plaque tournante du cybercrime ouest-africain.

4.

ANALYSE CRITIQUE DES MOYENS ET DISPOSITIFS ACTUELS

4.1. Insuffisance de la maitrise statistique sur la cybercriminalité

Une des problématiques centrales dans la lutte contre la cybercriminalité est la capacité à la mesurer et l'analyser quantitativement pour en tirer des photographies objectives. Une grande majorité des cybercrimes restent sous-rapportés et sous-comptabilisés, ce qui implique une prédominance du chiffre noir de la cybercriminalité.

De manière générale, le « chiffre noir de la criminalité » désigne l'ensemble des actes criminels commis dans un espace géographique donné et non portés à la connaissance des services de police et de justice. Il représente entre autres le nombre de crimes et délits qui ne feront l'objet ni d'une plainte auprès des services de Police ou de gendarmerie, ni d'une instruction par les services de justice. Dans le cas de la cybercriminalité, ce chiffre est particulièrement important et les outils statistiques utilisés ne répondent pas toujours aux exigences techniques de cette forme de criminalité. Ainsi, selon le FBI en 2009, entre 85% et 97% des crimes n'étaient même pas révélés. D'autres experts estiment qu'en dépit du niveau relativement évolué des outils et méthodes de collectes des statistiques en Europe, moins de 1% des infractions liées à la cybercriminalité parviennent au tribunal en Occident.[22]

En tout état de cause, tenter de mesurer la cybercriminalité à partir des seuls évènements enregistrés dans les registres des services d'application de la loi, aurait pour conséquence d'établir une perception sous-évaluée du phénomène. En effet, les statistiques fournies par la PLCC, le CI-CERT ou la DPEF ne donnent qu'une vision très partielle du phénomène et ne permettent pas de l'appréhender dans sa dimension évolutive ou dans ses mutations. Les variations observées dans les statistiques officielles ne sauraient rendre compte d'une évolution ou diminution des cybercrimes, mais devraient plutôt être interprétées comme une amélioration des capacités de prises en charge des infractions, induites par un accroissement des signalements faits par les victimes.

En outre, le système pénal ivoirien ne s'autoalimente pas, c'est-à-dire que pour qu'un service d'application de la loi ait connaissance d'une infraction, il a principalement besoin qu'elle lui soit rapportée par les victimes ou des témoins. De ce fait, le chiffre noir demeurera dans des proportions très importantes, car les cybercrimes sont difficiles à détecter par les victimes ou d'éventuels témoins. De plus, le faible niveau de sensibilisation et de connaissance des symptômes et autres implications techniques sont largement méconnues par les citoyens. Aussi, certaines victimes redoutent-elles l'impact d'une déclaration aux services judiciaires sur leur image, leurs affaires. De ce fait, les victimes ne jugent pas nécessaires de déclarer des actes qu'ils n'estiment pas si graves pour effectuer un signalement, etc. Par exemple, dans le secteur bancaire, les campagnes de spams, les tentatives d'intrusion ou de brute force, et certains événements de sécurité ne sont quasiment jamais rapportées, jusqu'au moment où un impact financier considérable est enregistré.

[22] https://www.crime-research.org/articles/sabad03_2004

En Côte d'Ivoire, le législateur a adopté une législation spécifique faisant obligation à tous les acteurs nationaux de signaler tous les incidents de cybersécurité dont ils sont victimes, mais cette obligation est très faiblement mise en œuvre pour diverses raisons.
Par ailleurs, on peut observer un manque d'uniformisation des qualifications retenues par les officiers de police judiciaires dans le traitement des plaintes et signalement en matière de cybercriminalité. En effet, l'appréciation et la qualification des faits portés à la connaissance des autorités d'application de la loi reste largement disparate et peut varier en fonction du niveau de compétence ou de compréhension technique de l'officier ou l'agent de police judiciaire. En conséquence, des faits identiques déclarés à deux services différents peuvent être taggués avec des index différents.
Enfin, l'absence de mutualisation des bases de données statistiques des différents services d'application de loi ne permet pas une détection efficace de ces écarts et mise en cohérence des différents chiffres.

4.2. Gouvernance pas suffisamment claire et précise

La réponse opérationnelle à la cybercriminalité par les services d'application de la loi (police et gendarmerie) n'a pas fait l'objet d'une véritable définition formelle précisant clairement les rôles, responsabilités et limitation et champs de compétences des différents acteurs. En effet, jusqu'à aujourd'hui, les services techniques de la police ou de la gendarmerie conduisent des investigations et procédures judiciaires liées à la cybercriminalité, indépendamment les uns des autres. A l'instar des technologiques du numérique, le cybercrime a une dimension transversale qui pose une véritable équation dans sa qualification et sa prise en charge. Un même cybercrime peut avoir à la fois une dimension purement technique (utilisation de logiciels malveillants), économique (gain financier), exploitation sexuelle des mineurs et déboucher sur des infractions liées aux trafics de stupéfiants (drogue) ou au terrorisme. Dans l'organisation actuelle, tant au niveau de la police que de la gendarmerie, les domaines de compétences sont définis en fonction du découpage territorial ou du type de criminalité. Cependant, le cas de cybercriminalité rend encore plus floues et imprécises les frontières entre les domaines de compétences, tels que définis traditionnellement. Dans la pratique, des cybercrimes sont reportés à l'un ou l'autre service en fonction de l'aspect le plus important pour la victime. En effet, dans le cas de cybercrimes dans le secteur bancaire, la police économique et financière sera plébiscitée, tandis que pour des cas liés à un cyberescroquerie, la PLCC sera saisie en priorité. Dans de nombreux cas, deux services différents sont saisis pour le même cybercrime, occasionnant une prise en charge partielle d'un aspect singulier du cybercrime par chacun des services, voire un chevauchement dans les investigations.
Aussi, la question de la compétence territoriale mérite-t-elle également d'être adressée dans le cadre de la lutte contre la cybercriminalité. Traditionnellement, la gendarmerie et la police ont des compétences géographiques spécifiques, mais ce principe est difficile à mettre en œuvre dans le cas de la cybercriminalité qui ignore les limites géographiques

tant nationales, qu'internationales. En Côte d'Ivoire, la lutte contre la cybercriminalité a été majoritairement portée par la police nationale depuis le début des années 2010. Cependant, la gendarmerie nationale se dote progressivement de capacités opérationnelles de lutte, ce qui remet plus que jamais d'actualité la question de la séparation et la limitation des champs d'intervention. En effet, dans le contexte local actuel, cette absence de gouvernance claire et formalisée au plus haut niveau représente un véritable point d'achoppement de l'action régalienne de l'Etat dans le cadre de la lutte contre la cybercriminalité.

Par ailleurs, la volonté de l'Etat Ivoirien de créer une agence nationale de la sécurité des systèmes d'Information devrait apporter quelques éléments de solution à cette question, mais pas suffisamment pour adresser complètement la question de la compétence et du périmètre d'action. En effet, l'Etat Ivoirien devrait capitaliser les acquis du modèle de gouvernance actuel, qui du reste règle une grande partie des difficultés liées à la collaboration inter organisations, qu'on peut observer dans d'autres modèles d'organisation d'agences nationales de la sécurité des systèmes d'information. Il existe également un risque d'accroitre le cloisonnement entre les forces vives et adopter une doctrine top-down strictement enfermée dans un cadre à forte connotation judiciaire, susceptible de freiner la collaboration volontariste des acteurs du secteur privé et de la société civile en matière de cybersécurité. Dans le contexte de la cybercriminalité, une nouvelle approche organisationnelle devrait être envisagée, afin de permettre à toutes les forces vives de jouer leur partition dans ce vaste chantier de manière harmonieuse et concertée.

4.3. Moyens de veille et de signalement insuffisants

Avec un système pénal dit non « self *starter* », c'est-à dire qui ne s'autoalimente pas et donc repose essentiellement sur les plaintes des victimes ou témoins, les dispositifs de signalement doivent être largement accessibles aux populations cibles. Avec l'essor du numérique, les mécanismes de signalement et d'enregistrement classiques de plaintes ne sont plus adaptés aux contexte de la cybercriminalité. Quelques dispositifs nouveaux de signalement ont été mis en place, mais restent peu accessibles et peu vulgarisés pour permettre des taux de saisine plus importants. En effet, bien que les populations aient la possibilité de faire des signalements en ligne via les comptes de médias sociaux de la PLCC, le principal moyen de saisine reste encore la plainte physique auprès de services compétents. Les nombreuses contraintes liées à cette procédure classique ne favorisent pas des signalements massifs et limitent les interactions avec les services compétents, exclusivement pour les cas les plus graves.

En outre, le nombre réduit de personnels affectés à la prise en compte des signalements et plaintes en matière de cybercriminalité entraine une priorisation dans le traitement des plaintes en fonction du niveau de gravité estimé par l'agent.

Par ailleurs, la police et la gendarmerie disposent de très peu voire pas de moyens de veille et patrouilles dans le cyberespace. Les quelques dispositifs de cyber patrouilles sont limités à l'observation des contenus publiés sur les groupes publics accessibles sur les forums et réseau sociaux dans le *clear web*[23]. Au niveau du CI-CERT, une veille minimale sur les campagnes d'exploitation de vulnérabilités connue est effectuée. Cependant, il n'existe pas de mécanismes systématiques de veille sur des places cybercriminelles d'intérêt.

4.4. Spécialisation insuffisante des magistrats

En tant que champ d'application spécifique du droit pénal, la cybercriminalité exige pour les magistrats une relative maitrise technique des mécanismes et modus operandi en plus des compétences juridiques. En effet, sans être des experts de l'investigation numérique et de la cybersécurité, les magistrats doivent tout de même disposer d'un bagage de connaissance technique de base suffisamment fourni, afin de mieux appréhender les implications juridiques d'une cyberinfraction. Pour l'heure en Côte d'Ivoire, il n'existe pas de mécanismes spécifiques de formation initiale ou continue et de spécialisation des magistrats en matière de cybercriminalité, comme c'est le cas pour la criminalité économique et financière ou les stupéfiants par exemple. Cette absence de profils de magistrats spécialisés dans le domaine de la cybercriminalité favorise une répression partielle des cyber infractions portées à la connaissance de l'appareil judiciaire. Par ailleurs, le nombre insuffisants de magistrats et le mode d'organisation de la profession oblige l'administration judiciaire à effectuer des rotations et des réaffectations régulières, afin de combler les déficits et assurer une couverture la plus large possible du territoire national. Dans un tel contexte de rotation des effectifs, des magistrats ayant acquis des compétences et connaissances basiques sur la cybercriminalité, n'ont pas suffisamment le temps de se spécialiser par la pratique dans ce domaine spécifique sur le long terme.

4.5. Faible traitement de renseignements criminels en matière de cybercriminalité

Le renseignement criminel est une approche de lutte contre la criminalité largement utilisée par les services de police, quand bien même le concept n'est pas officiellement adopté dans certains pays. En Côte d'Ivoire, la pratique du renseignement criminel est étendue à quasiment toutes les composantes des services de lutte contre la criminalité, notamment la police et la gendarmerie. De plus, la recrudescence des menaces terroristes a également conduit les services de lutte contre la criminalité à développer des capacités supplémentaires en matière de renseignement criminel, afin de collecter des informations sur les délinquants, tenir des registres d'empreintes digitales et/ou

[23] Le *clear web* correspond à toutes les pages indexées par les moteurs de recherche classiques et accessibles via les navigateurs web tels que Firefox, Google Chrome, Opera, etc.

d'échantillons d'ADN, conduire des enquêtes clandestines, y compris avec le concours d'informateurs.
Par ailleurs, l'usage de systèmes d'information dédié au renseignement criminel se mets en place progressivement avec le développement des capacités du centre de fusion et d'analyse de données de la DITT. En effet, des logiciels spécialisés opérés par des analystes de données et assistés de criminologues permettent d'apporter plus d'efficacité que les méthodes traditionnelles basées exclusivement sur la collecte de renseignement de documents papier et d'informateurs. L'usage de ces techniques et méthodes de renseignement pour identifier les nouvelles menaces posées par les délinquants ou pour établir des profils des délinquants ou des crimes existants est encore à ces balbutiements, mais se développe progressivement.
Cependant, très peu d'outils informatisés de renseignements criminels sont mis en œuvre dans le cadre de la lutte contre cette forme particulière de criminalité, qui est par nature ultradynamique et dont les preuves relativement volatiles.

4.6. Absence d'une politique criminelle nationale spécifique à la cybercriminalité

L'historique de la mise en place des mécanismes de lutte contre la cybercriminalité a montré que les réponses ont été apportées pour parer à l'urgence, sans une véritable stratégie globale en la matière. Si les premières actions de l'Etat à travers les acteurs opérationnels clés ont apporté des réponses concrètes aux problèmes que posaient cette nouvelle forme de criminalité à notre pays, force est de constater qu'au fil du temps, très peu de planification stratégique a été implémentée. Confinant la lutte contre la cybercriminalité à un ensemble d'actions et d'initiatives ad'hoc entreprises au gré des manifestations les plus visibles du phénomène. En tant que phénomène social inhérent à la société humaine, la criminalité dans son assertion la plus large est un fait normal, comme le soulignait Emile Durkheim dans *Les Règles de la Méthode Sociologique*.
Considérée sous cet angle, la criminalité ne peut être supprimée, mais plutôt appréhendée dans ses modes d'expression les plus variés, afin d'en contrôler au mieux les effets sur la société. De ce fait, lutter contre la cybercriminalité exige une action planifiée à travers laquelle l'État cherche à réagir contre le cybercrime. Cet ensemble planifiée de procédés préventifs et répressifs contre le crime est connu sous le concept de politique criminelle.
En Côte d'Ivoire, différents acteurs ont légitimement engagés des moyens de lutte contre la cybercriminalité, sans une véritable planification définissant un ensemble de stratégies ou des procédés au travers desquels l'État et la société organisent leurs réponses au problème de la criminalité. Bien que des jalons importants aient été établis, il en résulte à l'échelle nationale une réponse isolée, unilatérale, de tendance réactive dans laquelle prédomine à peine le caractère répressif de l'action de l'État. En effet, aucune véritable politique criminelle spécifique à la cybercriminalité n'a été mise en place, afin d'apporter une réponse globale et concertée à la hauteur des enjeux que représentent cette forme de criminalité particulière.

Comme toute politique publique, la politique criminelle doit tirer son essence de la tradition juridique du pays tout en prenant en compte les enjeux sociétaux et économiques, afin de garantir une mise en œuvre harmonieuse. La loi N°2013-451 relative à la lutte contre la cybercriminalité a posé les fondements juridiques de l'action pénale en matière de lutte contre la cybercriminalité, mais ne suffit pas à elle seule à définir une vision globale et concertée des objectifs à atteindre et de la manière dont ces objectifs doivent être atteints. En effet, le caractère spécifique de la cybercriminalité impose la définition d'une approche holistique qui se démarque de celles adoptées dans le cadre de la lutte contre les formes criminalité dites classiques. Il est nécessaire de définir un nouveau paradigme et mettre en cohérence, les ressources limitées dont dispose le pays, afin de maximiser l'efficacité de l'action de l'Etat, face à des menaces en constantes évolution.

4.7. Faible implication des intermédiaires techniques (FAI, FSI, etc.)

Avec l'essor du numérique, les intermédiaires techniques ont acquis un rôle capital dans lutte contre la cybercriminalité. Ils peuvent être regroupés en deux catégories d'acteurs, notamment : les fournisseurs de services de Télécommunications/TIC et les Prestataires techniques de services en ligne. En tant que fournisseurs des moyens techniques nécessaires aux activités en ligne, ces acteurs doivent être impliqués au premier plan dans l'élaboration des politiques publiques en matière de lutte contre la cybercriminalité et sécurisation du cyberespace national. Cependant, en l'absence d'une politique criminelle concertée, inclusive et spécifique en la matière, les intermédiaires techniques sont faiblement impliqués sur le chantier herculéens de lutte contre la cybercriminalité. Alors qu'ils devraient être de véritables partenaires engagés et proactifs dans la lutte, leur posture est résolument réactive et figée dans une relation entre donneur d'ordre (autorité judiciaire) et exécutant (intermédiaires techniques).
Quand bien même les intermédiaires techniques en général et les opérateurs en particulier sont soumis à des obligations légales clairement définies en matière de procédure pénale, il est nécessaire de repenser un nouveau modèle de coopération fondé sur une approche volontariste et citoyenne gagnant-gagnant. Dans une telle approche, les intermédiaires techniques deviendraient des acteurs proactifs en termes de signalement et prévention des cybercrimes, prolongeant ainsi l'action de l'autorité judiciaire dans les limites légales définies.

5.
PROPOSITIONS DE SOLUTIONS

AXE 1 : MIEUX CERNER LES CONTOURS DE LA CYBERCRIMINALITÉ

Proposition 1 : Mettre en place un centre d'études et recherches sur la cybercriminalité

L'exemple du Kenya est un cas d'école qui peut être repris et adapté au contexte de la Côte d'Ivoire, avec le Centre national de recherche sur la criminalité (NCRC – National Crime Research Centre). Il joue un rôle important en collectant massivement les données nationales relatives à la criminalité et en facilite leur accès et leur utilisation par les autorités nationales compétentes. Dans le court terme, une cellule de traitement de l'information spécifiquement dédiée à la cybercriminalité peut être mise sur pieds, avec pour mission la collecte et la normalisation des données ; afin de mettre à la disposition des autorités compétentes des informations d'aide à l'action. En tant que point central de collecte et d'analyse des données statistiques liées à la cybercriminalité, cette cellule sera en mesure de produire des informations sur les tendances, formes et mutations de la cybercriminalité, sur le sentiment d'insécurité numérique vécu par les populations, etc. La production de telles données qualitatives seraient d'une grande utilité pour orienter les efforts des différentes parties prenantes et utiliser de manière optimale les ressources disponibles. Par ailleurs, ce centre jouerait le rôle de pôle principal du renseignement criminel en matière de cybersécurité en compilant une évaluation nationale des menaces représentées par la cybercriminalité, à savoir rassembler et classer toutes les informations disponibles des principaux responsables de la délinquance, des préjudices qu'ils causent et de l'évolution vraisemblable de leurs agissements criminels. Ainsi, les études et analyses de ce centre mettraient en relief les menaces ou manifestations émergentes de la cybercriminalité susceptibles d'être évitées au moyen d'interventions à la source avant qu'elles ne deviennent un problème majeur.

Dans le long terme, les prérogatives et le champs d'action de cette cellule pourraient être étendus à toute la criminalité, comme c'est le cas au Kenya.

Proposition 2 : Mettre en place une plateforme nationale de signalement accessible en ligne 24/7 via une application mobile et un site web

L'insuffisance des moyens de signalement et les mécanismes actuels d'enregistrement de plaintes, contribuent incontestablement au faible nombre de déclarations liées à la cybercriminalité faites par les populations aux forces d'application de la loi. En effet, jusqu'à ce jour pour porter une affaire à la connaissance des autorités policières, la plainte physique reste le moyen privilégié, en dépit des énormes contraintes que cela comporte. Le temps nécessaire pour remplir les formalités administratives, les craintes légitimes ou non liées à la peur, la honte ou la gêne de déclarer certains faits, etc., sont autant de facteurs qui limitent la propension des populations à déclarer des infractions aux autorités compétentes. Des mécanismes nouveaux de signalement supprimant toutes ces barrières et contraintes doivent être mises en œuvre, afin de faciliter la communication entre les populations et les autorités judiciaires.

Avec un taux de pénétration de plus de 164,5% au 31 mars 2023[24], la téléphonie mobile représente en Côte d'Ivoire un excellent vecteur de communication entre l'Etat et les populations. A l'instar du NCRC qui a lancé en 2017 une application permettant aux citoyennes et aux citoyens kényans de signaler anonymement les crimes, la Côte d'Ivoire gagnerait à développer et vulgariser une telle application mobile dédiée au signalement des cybercrimes. En plus, d'être accessible via l'application mobile, une plateforme web pourrait également être associée, afin de permettre aux usagers de signaler anonymement des cybercrimes dont ils sont victimes ou dont ils ont connaissance. Cette plateforme de signalement permettra une importante collecte d'informations pertinentes pour dresser une cartographie des différentes formes de cyber infractions, mais également d'évaluer à minima le sentiment d'insécurité vécu par les populations.

[24] https://www.artci.ci/index.php/marches-regules/10-observatoire-du-secteurs-des-telecoms/sevice-mobile/89-abonnes-service-mobile.html

Proposition 3 : Définir un référentiel taxonomique national des cybercrimes

Avec la création du Centre de Traitement des Informations Policières (CTIP), la Côte d'Ivoire s'est dotée de moyens et ressources techniques nécessaires pour l'exploitation du système d'information policière de l'Afrique de l'Ouest (SIPAO) conçu par Interpol et financé par l'Union européenne. Le SIPAO est un système tridimensionnel qui permet de créer dans chaque pays un système de collecte national, de centralisation et de partage électronique de données policières entre les services chargés de l'application des lois. Ensuite, il dispose d'une plateforme de partage de données au niveau régional et ouvre un accès directe aux bases de données mondiales d'Interpol via son réseau de communication sécurisé.

Cette étape constitue un pas important vers la centralisation des données policières liées à criminalité en général. Cependant, le cas de la cybercriminalité mérite une attention singulière, afin de prendre en compte les spécificités de cette forme de criminalité ultradynamique. En effet, il est impératif de définir un registre national comprenant une taxonomie claire, compréhensible et admise par tous les acteurs impliqués dans la lutte contre la cybercriminalité.

Avec la multiplicité des formes et modalités d'expression de la cybercriminalité, un registre nationale aura l'avantage de définir un vocabulaire commun à tous les acteurs, afin de réduire les différences de qualification et d'indexation des faits constitutifs d'infractions de cybercriminalité, d'un service à un autre.

De plus, un tel registre national faciliterait grandement l'adoption et l'exploitation optimale du SIPAO par tous les services d'application de la loi.

AXE 2 : FÉDÉRER LES EFFORTS ET ENGAGER TOUS LES ACTEURS CLÉS

Proposition 4 : Mettre en place une plateforme de données ouvertes liées à la cybercriminalité

Dans le domaine de la lutte contre la cybercriminalité comme dans bien d'autres secteurs, l'accès aux données publiques par les parties prenantes (société civile, citoyens, chercheurs, etc.) reste extrêmement difficile. Une redéfinition de la culture de l'information est nécessaire, afin de tirer profit des grandes quantités de données que peuvent générer les services d'application de la loi en général, pour proposer des solutions innovantes et adaptées aux évolutions technologiques. En effet, la disponibilité, l'accessibilité et la primeur à l'information doivent être établis en véritables principes sacro-saints, afin de favoriser l'engagement de toutes les forces et entrainer une émulation positive dans les propositions de solutions.

La mise en place d'une plateforme de données ouvertes liées à la cybercriminalité peut constituer un véritable catalyseur de la recherche et du développement de solutions tant sur le plan technologique, que sur le plan socio-criminologique. En effet, un accès libre aux données liées à la cybercriminalité permettrait à toutes les parties intéressées de tirer des enseignements, analyser les tendances et difficultés, afin de proposer des solutions innovantes et originales.

A l'heure du numérique, l'Etat seul ne saurait proposer valablement des solutions viables aux problèmes que posent la cybercriminalité. Les services d'application de la loi ne sont pas en mesure de développer toutes les solutions techniques nécessaires pour appréhender et lutter contre la cybercriminalité. En ce sens, un partage de l'information technique, de l'état de l'art et des savoir-faire techniques du secteur privé et de celui de la recherche scientifique serait plus que bénéfique pour apporter des solutions efficaces. Des partenariats stratégiques devraient être établis entre les startups, les PME et grandes entreprises privées du secteur des technologies et les centres universitaires de recherche, afin d'identifier des axes de développement et d'innovation en la matière.

Proposition 5 : Renforcement de la plateforme de lutte contre la cybercriminalité

La plateforme de lutte contre la cybercriminalité devrait être étendue pour intégrer toutes les parties clés notamment la gendarmerie, la douane, le CENTIF, le PPEF, etc. En effet, la PLCC est un excellent modèle de coopération nationale qui a montré la viabilité de son modèle, depuis sa mise en œuvre jusqu'à ce jour. Dans le contexte d'une lutte asymétrique emmenée par les mutations ultra dynamiques des formes de la cybercriminalité, cette nouvelle approche de coopération est un modèle à renforcer et inscrire dans un processus d'amélioration continue. A terme, la PLCC devrait être transmuée en véritable task-force nationale d'élite en matière de lutte contre la cybercriminalité, mettant en œuvre la puissance publique dans toutes ses composantes opérationnelles. Avec sa vingtaine de personnels actuel, ses effectifs devraient être renforcés à travers l'élargissement de la convention de partenariat portant création de la plateforme de lutte contre la cybercriminalité à d'autres services (gendarmerie, douanes, etc.). Par ailleurs, un déploiement des effectifs de la PLCC à travers les grandes villes du pays est à envisager, afin de rapprocher le services des population et faciliter la prise en compte des signalements de cybercriminalité.

Proposition 6 : Créer un pôle pénal spécialisé en matière de cybercriminalité

La justice doit s'adapter aux évolutions de la criminalité à travers des juridictions spécialisées. L'Etat Ivoirien s'est doté à travers la Loi N° 2022-193 25du 11 mars 2022 portant création, compétence,
organisation et fonctionnement du pôle pénal économique et financier, d'une juridiction pénale de premier degré, spécialisée en matière de délinquance économique et financière, et chargée de la poursuite , de l'instruction et du jugement des infractions relevant de sa compétence. Ce pôle spécial a compétence pour connaitre également les infractions économiques et financières commises par le biais de systèmes d'information et de communication. Même s'il dispose de prérogatives statutaires pour la lutte contre la cybercriminalité, l'accent semble avoir été mis sur les aspects économique et financier. Le pôle pénal économique et financier peut être un excellent tremplin dans la dynamique de spécialisation des magistrats en matière de lutte contre la cybercriminalité, à travers le développement d'un pool de magistrats spécialisés en la matière.
Cependant, la création d'un pôle pénal ou à minima d'un parquet spécialisée dans la cybercriminalité devrait être une priorité stratégique de l'Etat Ivoirien , afin de renforcer le suivi et la lutte contre les crimes cybernétiques dans leur grande diversité.

[25] https://habg.ci/documents/LOI%20n%C2%B0%202022-190%20du%2011%20MARS%202022.pdf

Proposition 7 : Initier les acteurs des services d'application de la loi à la lutte contre la cybercriminalité dès les écoles de formation (Magistrats, Policiers, gendarmes)

La question du développement des capacités des acteurs opérationnels de lutte contre la cybercriminalité représente un enjeu capital, pour la lutte contre la cybercriminalité. La pénurie mondiale de compétences en cybersécurité, n'épargne pas les services d'application de la loi. En Côte d'Ivoire, cette tendance pourrait être résorbée par l'intégration de modules d'initiation et de formation à la sécurité numérique et lutte contre la cybercriminalité dans les cursus des écoles nationales de formation (INFJ, ENP, ENG, etc.). En effet, le CI-CERT a développé un programme complet de formation à la sécurité dénommé DIGISEC (Digital Security Classroom), qui pourrait être adapté et intégré dans les curricula de formation des écoles nationales de formation INFJ (magistrats), Ecole Nationale de Police (ENP), Ecole Nationale de Gendarmerie (ENG), etc. Un cursus de formation des formateurs pourrait être spécifiquement développé, afin de fournir à chaque corps, les moyens de donner les bases théoriques et techniques en matière de lutte contre la cybercriminalité. Des cursus de spécialisation pour les enquêteurs seraient ensuite mis en œuvre en fonction des orientations et besoins opérationnels.

Proposition 8 : Mettre en œuvre un modèle de contrôle des circuits financiers entre la BCEAO et les autorités de régulation des communications électroniques et de la cybersécurité

Le traditionnel cloisonnement entre les autorités de régulation des marchés financiers et des télécommunications s'avère être une véritable aubaine pour les cybercriminels qui utilisent les insuffisances de ce modèle complètement dépassé eu égard à la convergence quasi-totale des services financiers et plateformes technologiques modernes. En effet, il est nécessaire de créer une passerelle nationale de coopération formalisée entre les autorités de régulation du secteur financier (BCEAO, CENTIF, etc.) et les autorités de régulation en charge de la cybersécurité (ARTCI). Cette plateforme contribuerait à assurer un suivi plus efficace des flux et circuits financiers illicites et contribuer efficacement à réduire les gains des acteurs malveillants, à travers le partage de renseignements et des actions communes d'investigations.

Proposition 9 : Organiser un événement annuel d'information et de sensibilisation à la sécurité numérique en collaboration avec les FAI

La sensibilisation est assurément un des leviers majeurs pour la lutte contre la cybercriminalité. Aucune approche essentiellement répressive ne saurait apporter des réponses viables aux problèmes que posent la cybercriminalité. Ceci est d'autant plus vrai dans le contexte socio-économique Ivoirien marqué par un faible taux d'alphabétisation et une ignorance des enjeux de la cybercriminalité et règles basiques de bonne hygiène numérique. Les prestataires techniques en général et les fournisseur d'accès à Internet ont un rôle capital à jouer dans cette dynamique globale de sensibilisation et de prévention. L'Etat Ivoirien devrait institutionnaliser en collaboration avec tous les fournisseurs d'accès à Internet, un forum commun regroupant les services d'application de la loi, les services techniques opérationnels (CI-CERT, ANSSI, etc.) et les FAI. Ce forum réaliserait au moins un événement national annuel grand public de sensibilisation et de prévention contre la cybercriminalité. En effet, le rôle des fournisseurs d'accès à internet devrait être renforcé, afin de faire de la lutte contre la cybercriminalité un véritable argument commercial témoignant de leur engagement citoyen à fournir aux populations, un cyber environnement sécurisé et sain.

Les moyens de communication dont ils disposent peuvent constituer un excellent canal pour atteindre le maximum de cibles et créer une véritable relation de confiance entre les utilisateurs et les services d'application de la loi à travers un véritable partenariat gagnant-gagnant. Jusqu'à ce jour, très peu voire aucune campagne de sensibilisation d'envergure nationale n'a jamais été réalisée, dans le cadre de la lutte contre la cybercriminalité.

A l'instar des règles de sécurité routière qui font quasiment partie intégrante de notre conscience collective, les acteurs devraient déployer des efforts conjoints pour élever le niveau de conscience face aux dangers et risques de sécurité encourus en cas de non-respect de certains règles de base dans le cyberespace.

AXE 3 : STRUCTURER LA RIPOSTE ET RATIONNALISER LES RESSOURCES

Proposition 10 : Développer une stratégie nationale de lutte contre la cybercriminalité

La cybercriminalité revêt de nombreuses formes et présente un caractère transversal unique. En tant que phénomène social échappant complètement aux limites des formes traditionnelles de criminalité, elle impose de définir des mécanismes et stratégies de réponse originaux et adaptés à l'ampleur de la menace. Il est indispensable de définir une stratégie nationale de lutte contre la cybercriminalité qui fixe les objectifs réalistes à atteindre, ainsi que les moyens à mettre en œuvre et les principes généraux de l'action concertée de tous les acteurs clés. Le développement de stratégies efficaces devra répondre à des exigences méthodologiques éprouvées à même de produire des résultats probants.

A ce titre, les travaux de l'Office des Nations Unis Contre la Drogue et le Crime (ONUDC) fournissent une excellent base opérationnelle dans « RÉFÉRENTIEL STRATÉGIQUE DE LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE POUR L'ÉLABORATION DE STRATÉGIES À FORT IMPACT[26] ». L'approche méthodologique proposée dans ce référentiel peuvent servir de boussole, pour l'élaboration d'une stratégie nationale de lutte contre la cybercriminalité basée sur les principes dits des 4P suivants :

- **PRÉVENTION** : prévenir toute (ré)infiltration des communautés, de l'économie et des institutions politiques par la cybercriminalité. Ce principe vise à renforcer la résistance à la cybercriminalité organisée, en lui refusant la possibilité de pénétrer dans la société.
- **POURSUITES** : poursuivre les groupes cybercriminels organisés et leurs gains illicites, à travers des activités qui augmentent les coûts et les risques pour les entreprises. Ce principe vise à dégrader et à perturber l'économie de la cybercriminalité organisée.
- **PROTECTION** : protéger les personnes vulnérables et les victimes à l'égard de tout (nouveau) préjudice. Ce principe reconnaît les dommages et les préjudices que la cybercriminalité organisée inflige aux femmes et aux hommes en privilégiant une approche centrée sur la victime qui intègre des considérations relatives aux droits humains et au genre.
- **PROMOTION** : promouvoir des partenariats et de la coopération à tous les niveaux, y compris au-delà des frontières internationales – une démarche mobilisant l'ensemble de la société. Ce principe, qui est au cœur même de la Convention contre la criminalité organisée, souligne l'importance des partenariats aux niveaux local, national et international, et de la collaboration entre les secteurs public, non gouvernemental et privé.

[26] https://www.unodc.org/documents/organized-crime/tools_and_publications/Strategies_Toolkit/Strategy_Toolkit_FR.pdf

CONCLUSION

En dépit d'un relatif intérêt pour la question de la cybercriminalité depuis ces derniers années, les acteurs de l'économie numérique (pouvoirs publics, secteur privés, société civile) ne semblent pas avoir pris la pleine mesure des enjeux liés aux mesures nécessaires à mettre en œuvre pour contrôler le phénomène. L'Etat ivoirien a entrepris plusieurs réformes et engagés plusieurs chantiers d'ordre structurel, organisationnel et opérationnel pour fournir un cyberespace qui inspire confiance aux utilisateurs et aux investisseurs. Cependant, le manque d'actions concertées et coordonnées entre tous les acteurs clés, ne permet pas d'appréhender la question de la lutte contre la cybercriminalité dans toutes ses dimensions, notamment épistémologique, axiologique, cognitive. Entre 2009 et 2022, le préjudice financier direct déclaré à la PLCC et au CI-CERT s'élève à un peu plus de soixante (60) milliards FCFA, issus du traitement de 30.029 dossiers de cybercriminalité. Cependant, le fait que seulement 5% des suspects interpellés par suite d'une déclaration aux autorités judiciaires et dont 3% seulement aboutissent à un déféremment des suspects impliqués devant le parquet, indique l'extrême difficulté que pose l'identification des cybercriminels. Par ailleurs, le chiffre noir de la cybercriminalité s'établit dans des proportions de plus en plus abyssales et laisse entrevoir l'émergence de nouvelles formes de cybercriminalité toujours plus évoluées et au potentiel de nuisance plus grand.

Les résultats des analyses et conclusions de ce rapport ne sauraient être considérées comme une finalité, mais plutôt comme une base de réflexion et de proposition pour adresser sous un angle nouveau, la question de la lutte contre la cybercriminalité.

Notre souhait est d'encourager la discussion et stimuler la réflexion sur les moyens et mesures à mettre en œuvre pour proposer un cyber environnement sain, gage de sécurité et de tranquillité pour les utilisateurs. En effet, dans un société à venir du tout ou presque numérique, la question de lutte contre la cybercriminalité et plus largement celle de la cybersécurité doivent être au cœur des politiques nationales de développement économique et social.

Dans la continuité des propositions formulées dans le présent ce rapport, les réflexions devraient être poursuivies en adressant de manière détaillées les différents axes suivants :

- Développement de modèles innovants de collaboration entre le secteur public et le secteur en matière de lutte contre la cybercriminalité et cybersécurité
- Développement des compétences en matière d'investigation numérique à travers la formation initiale et continue et la spécialisation des acteurs judiciaires
- Développement de la sensibilisation et de l'engagement citoyen, pour une action concertée de renforcement de la confiance numérique.

Bibliographie

AFFAGNON, Q. (s.d.). Cybercriminalité au Bénin: menaces, lacunes juridiques et pouvoir.

AKADJE Ahiouré Mathieu, A. J. (2022, Octobre). Cybercriminalité et Banques en Côte d'Ivoire. *REVUE SEMESTRIELLE ET SCIENTIFIQUE FONDEE PAR LE GUREP - Spécial N°005*.

Atta-Asamoah, A. (2009). Understanding the West-African cybercrime process.

AZI, W. J. (2021, Juin). Perceptions favorables de la cyberescroquerie et des réseaux cyberescrocs chez des jeunes. *Revue Africain de Criminologie - Revue Semstrielle N°21*, p. 66.

LEBROGNE-TAHIRI, C. (2022). Université et Nouvelles en Afrique de l'Ouest francophone, passé, présent et avenir.

MSHA, P. (2002, Juillet). Internet en Afrique subsaharienne: acteurs et usages, datation et acquisition.

Sociales, C. I. (2017). *Paysage de la migration en Cöte d'Ivoire.* Paris: Editions OCDE.

Webographie

1. https://www.afrik.com/l-internet-en-cote-d-ivoire-n-est-pas-un-effet-de-mode
2. https://doi.org/10.1787/9789264277090-6-fr
3. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_f.pdf
4. https://www.cicert.ci/index.php/publications/rapports-d-activites
5. https://www.artci.ci/index.php/publications/rapports-d-activites.html
6. https://horizon.documentation.ird.fr/exl-doc/pleins_textes/pleins_textes_7/b_fdi_55-56/010021302.pdf
7. https://transition.fcc.gov/Reports/tcom1996.pdf

Contacter l'auteur de cette publication : vladimiraman@gmail.com | www.hacktu.ci |