GROUPE DE RECHERCHE
ET D'INFORMATION
SUR LA PAIX ET LA SÉCURITÉ

467 chaussée de Louvain
B – 1030 Bruxelles
Tél. : +32 (0)2 241 84 20
Courriel : admi@grip.org
Internet : www.grip.org
Twitter : @grip_org
Facebook : GRIP.1979

Le GRIP bénéficie du soutien du Service de l'Éducation permanente de la Fédération Wallonie-Bruxelles.

NOTE D'ANALYSE – 19 novembre 2019

MÉCHINAUD Coline, *L'Afrique de l'Ouest dans le cyberespace : enjeux de sécurité et de souveraineté*, Note d'Analyse du GRIP, 19 novembre 2019, Bruxelles.

https://www.grip.org/fr/node/2852

NOTE D'ANALYSE

L'Afrique de l'Ouest dans le cyberespace : enjeux de sécurité et de souveraineté

Par **Coline Méchinaud**

19 novembre 2019

Résumé

Les cybermenaces sont devenues en quelques années des enjeux géopolitiques majeurs et une préoccupation grandissante pour de nombreux États. Les menaces terroristes et l'instabilité croissante dans le Sahel ont cependant retardé la prise de conscience dans la sous-région ouest-africaine, de telle sorte que la réflexion sur le numérique a souvent été cantonnée à une simple lutte contre une cybercriminalité. Cette Note d'Analyse procède à une revue des divers enjeux de sécurité et de souveraineté liés au cyberespace pour les États d'Afrique de l'Ouest ; soit des sociétés qui connaissent un essor numérique extrêmement rapide. Ce travail se base notamment sur des enquêtes de terrains et des entretiens menés au Sénégal, au Ghana, en Côte d'Ivoire et au Niger.

Abstract

Cyberspace: Security and sovereignty challenges in West Africa

Within a few years, cyberthreats have become a major geopolitical issue and a growing concern for many States. However, the West African context and the pressing threats to territorial integrity in the Sahel region have delayed the awareness in the sub-region, so that the policy concerns have been mostly limited to the fight against cybercrime. In the context of the rapid digital growth in West African States, this note analyses the diverse implications of cyberspace in terms of security and sovereignty. This work is partially based on interviews and fieldworks conducted in Senegal, Ghana, Côte d'Ivoire and Niger.

Introduction

Lors du récent Appel de Paris pour la confiance et la sécurité dans le cyberespace, de nombreux États, entreprises et organisations ont réaffirmé l'importance de la cybersécurité dans le monde actuel :

> « *Le cyberespace joue désormais un rôle capital dans tous les aspects de notre vie ; il relève de la responsabilité d'un grand nombre d'acteurs, chacun dans son domaine propre, de le rendre plus fiable, plus sûr et plus stable*[1]. »

Cette question, devenue primordiale pour les grandes puissances, peut sembler éloignée des priorités des États ouest-africains. Alors que le contrôle des territoires nationaux et l'exercice plein et entier des fonctions régaliennes restent problématiques dans certaines zones de la sous-région, il peut en effet paraître peu judicieux d'ériger la cybersécurité en enjeu prioritaire. Pourtant la question de la cybersécurité en Afrique de l'Ouest ne se limite pas à des arnaques et escroqueries en ligne, qui viseraient uniquement des Occidentaux. L'augmentation exponentielle de la couverture Internet mobile et la multiplication des grands projets liés au numérique offrent à la sous-région des opportunités considérables en termes de développement. Celles-ci s'accompagnent de risques grandissants et diversifiés, aux conséquences déjà importantes en termes économiques, sociétaux et sécuritaires.

Les États d'Afrique de l'Ouest ont aujourd'hui pris conscience de leur vulnérabilité et de l'importance d'acquérir la maitrise de leur espace numérique. L'adoption de la convention sur la cybersécurité et la protection des données à caractère personnel[2] – dite Convention de Malabo – par l'Union africaine en 2014 et les récents développements législatifs et opérationnels de la Côte d'Ivoire, du Sénégal ou encore du Burkina Faso, en ont été les premiers signes. Plus récemment, l'inauguration de l'École nationale à vocation régionale (ENVR) de cybersécurité de Dakar, et l'accent mis sur ce thème lors des deux dernières éditions du Forum international sur la paix et la sécurité en Afrique au Sénégal ont démontré un intérêt croissant pour le sujet.

Dans ce contexte, cette Note d'Analyse se penche sur les différents enjeux liés au cyberespace pour les États d'Afrique de l'Ouest. Elle s'intéresse tout d'abord à la cybercriminalité et l'utilisation d'Internet à des fins terroristes, enjeux majeurs de sécurité intérieure et transfrontalière. Elle examine ensuite la question sous l'angle de la conquête par les États de leur « *souveraineté numérique* ». Si ce concept n'est pas encore bien défini et qu'il engage des acteurs multiples, le contrôle du cyberespace prend une place de plus en plus centrale dans les relations internationales et les rapports entre les secteurs public et privé. La présente note dresse finalement un état des lieux des avancées et des principales difficultés rencontrées, puis formule des pistes de recommandations.

---

1. « Appel de Paris pour la confiance et la sécurité dans le cyberespace », 12 novembre 2018.
2. Voir le texte officiel de la *Convention sur la cybersécurité et la protection des données à caractère personnel de l'Union africaine*.

Elle a pour objectif premier de démontrer la nécessité, pour les États ouest-africains et leurs partenaires, d'accorder une place majeure à ces questions dans leurs politiques sécuritaires et économiques, afin d'éviter que le cyberespace ne devienne un nouveau vecteur d'instabilité dans une sous-région en proie à de nombreuses difficultés.

1. Des enjeux sécuritaires majeurs à court et long termes

1.1. La cybercriminalité, véritable frein au développement de la sous-région

La cybercriminalité ouest-africaine a longtemps été considérée comme limitée aux arnaques aux sentiments et autres escroqueries relativement simples, visant des particuliers occidentaux. Si les escroqueries sur Internet restent effectivement majoritaires, elles sont de plus en plus diverses (les arnaques sentimentales côtoyant aussi celles aux achats en ligne, aux bourses d'études, etc.). Elles sont aussi désormais talonnées par de nouvelles infractions comme la fraude au porte-monnaie électronique, l'accès frauduleux à des systèmes informatiques (visant souvent les entreprises de transfert d'argent telles Western Union ou Money Gram) ou encore l'enregistrement illégal de communications privées aussi appelé « sextorsion[3] ». Cette diversification des infractions s'accompagne d'une montée en puissance d'une partie des cybercriminels ouest-africains qui opèrent en groupes structurés, partagent leurs techniques et achètent des outils et logiciels malveillants sur les darknets[4]. Un rapport publié par Interpol et Trend Micro brosse le portrait de ces « *cybercriminels avancés* » qui ont mis au point des mécanismes complexes pour opérer des « *arnaques au président* »[5] et de la fraude aux remboursements d'impôts, en ciblant principalement les États-Unis[6].

Ces attaques ont un impact économique conséquent sur le développement des États de la sous-région. Si les pays occidentaux francophones et les États-Unis restent les cibles privilégiées, les entreprises et particuliers d'Afrique de l'Ouest sont de plus en plus victimes de ces infractions. La Police nationale de Côte d'Ivoire a par exemple enregistré depuis 2013 une hausse constante des victimes de cybercriminalité résidant en Côte d'Ivoire dans ses enquêtes.

3. Voir les rapports d'activité de la DITT de la Police nationale de Côte d'Ivoire, pour les années 2015 et 2016.
4. Un darknet est un réseau superposé qui utilise des protocoles spécifiques intégrant des fonctions d'anonymat. Le contenu de ces darknets, appelé le Dark Web, n'est donc pas référencé sur les moteurs de recherche classiques. Du fait de leur anonymat renforcé, les darknets abritent un grand nombre de plateformes vendant des biens et services illicites.
5. La « *fraude au président* » ou escroquerie des faux ordres de virement sont le fait d'escrocs qui convainquent le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.
6. « La cybercriminalité en Afrique de l'Ouest prête pour un marché souterrain », *Trend Micro et Interpol*, mars 2017.

Pour l'année 2016, elle a estimé un préjudice lié à la cybercriminalité d'environ 1,8 milliard FCFA (plus de 2,5 millions EUR) dans le pays, causé en grande partie par la multiplication des fraudes aux moyens de paiement électroniques et par l'augmentation des infractions entre pays africains[7]. Les banques de la sous-région, peu protégées contre la cybercriminalité, sont régulièrement victimes d'attaques[8].

Au préjudice provoqué par ces infractions s'ajoutent, pour certains États, des pertes financières liées au manque de confiance dans leur économie digitale. La méfiance des banques et des investisseurs envers l'espace numérique de pays tels que le Nigéria, et dans une moindre mesure la Côte d'Ivoire, ne cesse de croître et constitue un sérieux frein au développement. Au Nigéria, les pertes financières annuelles liées à la cybercriminalité ont été évaluées à plus de 600 millions USD en 2017[9], année marquée par un nombre particulièrement important d'attaques. Dans des pays faisant face à une explosion démographique et aux attaques de nombreux groupes terroristes, de telles pertes financières représentent une réelle menace pour la paix et la stabilité[10].

Au-delà du préjudice économique, les attaques contre des sites gouvernementaux ou des entités tant publiques que privées ont un fort potentiel déstabilisateur. Une large part des pertes subies par le Nigéria en 2017 sont en effet dues à des attaques visant des sites gouvernementaux. En outre, de nombreuses institutions publiques sont régulièrement visées dans la sous-région : la Banque centrale des États d'Afrique de l'Ouest (BCEAO) a ainsi récemment été l'objet d'une tentative d'attaque de grande ampleur[11]. Le manque de protection des systèmes d'information des sites publics ou privés ouest-africains explique qu'ils soient des cibles faciles et parfois des victimes collatérales des *botnets* (réseaux d'ordinateurs infectés) utilisés pour des attaques globales en déni de service (DDoS)[12].

Les effets de ces attaques sur des pays ayant un réseau Internet faiblement protégé et des infrastructures peu résilientes sont démultipliés, comme cela a pu être constaté lors de l'utilisation du malware Mirai[13] contre le Liberia, qui a paralysé une grande partie des services Internet du pays[14].

---

7. Rapports d'activité de la DITT de la Police Nationale de Côte d'Ivoire, pour les années 2015 et 2016.
8. « Afrique de l'Ouest : les banques ripostent face à la cybermenace », *La Tribune*, 8 avril 2019.
9. Serianu, Africa Cyber Security Report 2017, « Demistifying Afica's Cybersecurity Poverty Line ».
10. Voir Julien Dechanet, Melissande Ludman, Clément Rossi, « Afrique de l'Ouest : le nouveau défi de la cybersécurité », *CEIS*, avril 2017.
11. Osiris, « Cyberattaque en Afrique de l'Ouest : la BCEAO déjoue un 'assaut' » de taille », 14 janvier 2019.
12. Une attaque en déni de service ou en déni de service distribué (ou DDoS pour Distributed denial of service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou de dégrader fortement le fonctionnement fortement du service.
13. Logiciel malveillant qui transforme des ordinateurs utilisant le système d'exploitation Linux en bots contrôlés à distance, formant alors un *botnet* utilisé notamment pour réaliser des attaques à grande échelle sur les réseaux.
14. « Afrique de l'Ouest : le nouveau défi de la cybersécurité », *CEIS*, avril 2017.

Ce manque de protection des systèmes d'information et la volonté affichée de plusieurs États de numériser un grand nombre de services publics (voir notamment le projet Sénégal Numérique 2016-2025[15]) laissent craindre l'utilisation de ces moyens par les groupes terroristes présents dans la sous-région.

1.2. Cyberespace et terrorisme, un nouvel outil d'influence pour les groupes armés ouest-africains ?

L'utilisation d'Internet à des fins terroristes, parfois appelé cyberdjihadisme quand elle qualifie les pratiques en ligne des groupes prônant un djihadisme violent[16], regroupe les questions de propagande idéologique, de recrutement, de financement ou d'organisation au moyen de technologies informatiques. Ce terme recouvre des niveaux de compétences extrêmement divers dans l'utilisation des technologies. Il est possible de distinguer par exemple l'utilisation des réseaux informatiques comme moyens de communication, notamment pour la propagande, le recrutement ou comme plateforme opérationnelle de l'utilisation de technologies permettant un anonymat avancé sur des marchés souterrains mondialisés.

Les risques immédiats en Afrique de l'Ouest semblent davantage liés à la première catégorie, l'utilisation des technologies comme de nouveaux médias. L'essor rapide de la couverture Internet mobile dans la sous-région[17] a en effet contribué à faciliter la communication et l'organisation de la formation au combat et des attaques. Le récent procès de 29 membres d'un réseau terroriste au Sénégal a démontré l'importance nouvelle d'applications comme la messagerie *Telegram* dans un pays auparavant préservé de la radicalisation grâce à ses puissantes confréries soufies[18].

La propagande sur Internet se modernise également. Depuis 2015, Boko Haram et Al-Qaïda au Maghreb islamique (AQMI) reprennent à leur compte certains des codes introduits par État islamique (EI). Les traditionnelles vidéos statiques sont remplacées par des productions réalisées de manière quasi professionnelle, composées de chants djihadistes et d'images de combattants en treillis[19]. Plusieurs attaques ont été accompagnées d'un véritable plan médiatique incluant une communication en direct lors des combats et l'utilisation de multiples réseaux sociaux[20].

15. Plan d'actions qui prévoit entre autres choses la mise en ligne de 40 % des services administratifs.
16. Papa Gueye, *Criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles*, Dakar : L'Harmattan Sénégal, 2018.
17. Fin 2017, on comptait 176 millions d'abonnés uniques dans la sous-région avec un taux de pénétration global des abonnés atteignant les 47 %, soit 28 % de plus qu'en 2010. Les dynamiques démographiques accélèrent cette évolution, beaucoup de jeunes adultes allant ouvrir des abonnements dans les années à venir et le taux de pénétration global des abonnés devrait atteindre les 54 % en 2025. Voir « L'économie mobile de l'Afrique de l'Ouest », *GMSA*, 2018.
18. « À Dakar, 29 djihadistes présumés et un projet de califat en procès », *Le Monde*, 11 avril 2018.
19. « Attentats au Burkina, il y'a une sorte de compétition entre AQMI et l'EI », *Libération*, 16 janvier 2016.
20. « Attentats à Ouagadougou : AQMI adopte les codes de l'État Islamique », *Le Monde*, 18 janvier 2016.

La médiatisation et l'émotion mondiale provoquée par les vidéos de l'enlèvement des lycéennes de Chibok par Boko Haram (en 2014) ont montré à quel point ces nouvelles méthodes étaient efficaces pour un groupe voulant réaffirmer son influence et attirer de nouvelles recrues[21].

De manière générale, l'adoption massive et relativement incontrôlée des réseaux sociaux par les jeunes d'Afrique de l'Ouest offre de nouvelles opportunités particulièrement inquiétantes pour les groupes armés actifs dans la région. Ces plateformes, pour l'instant peu surveillées, leur permettent de diffuser leurs contenus à grande échelle et de toucher des publics nouveaux. Il existe quelques rares initiatives visant à lutter contre les contenus terroristes en ligne, notamment au Sénégal[22], mais les forces de l'ordre souffrent d'un manque significatif de moyens et de formation pour enquêter sur ces nouveaux médias.

À l'inverse, l'utilisation des nouvelles technologies à des fins de financement ou d'armement par les différents groupes armés actifs dans la sous-région n'est pas comparable à celle des groupes agissant au Moyen-Orient[23] et ne doit pas être surestimée. Il est à ce jour impossible d'affirmer que des technologies permettant un anonymat avancé, comme les cryptomonnaies[24] ou le Darknet, soient utilisées de manière conséquente et régulière par les groupes terroristes ouest-africains.

Alors qu'au Moyen-Orient plusieurs groupes tentent de lancer des campagnes de financement en cryptomonnaies[25], il n'existe jusqu'à présent aucun exemple de leur utilisation en Afrique de l'Ouest.

Malgré l'essor de la couverture Internet, le débit reste particulièrement faible dans la bande sahélienne et rend probablement l'utilisation de ces technologies (et notamment du réseau TOR[26]) difficile. Le niveau de maîtrise des outils informatiques est aussi moins avancé dans les groupes de la sous-région que dans ceux qui sont présents au Moyen-Orient.

---

21. « Jihad : La cyber-guerre est déclarée », *Jeune Afrique*, 28 janvier 2015.
22. Le Sénégal a lancé une plateforme similaire à la plateforme de signalement française Pharos et a pris part un récent appel de Christchurch contre l'extrémisme et le terrorisme en ligne, voir « Macky Sall s'engage dans la lutte contre le terrorisme en ligne », *Jeune Afrique*, 16 mai 2019.
23. Le groupe État islamique (EI) et le Hezbollah ont notamment des capacités technologiques avancées et utilisent des techniques permettant l'anonymat dans plusieurs domaines (financement, recrutement).
24. Une cryptomonnaie est une monnaie émise de pair à pair, sans nécessité de banque centrale, utilisable au moyen d'un réseau informatique décentralisé.
25. Steven Stalinsky, « The Coming Storm: Terrorists using Cryptocurrency », *MEMRI*, 21 août 2019. Voir également Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston « Terrorist Use of Cryptocurrency: Technical and Organizational Barriers and Future Threats », *RAND Corporation*, 2019.
26. Tor est un réseau informatique superposé mondial et décentralisé. Il se compose d'un certain nombre de serveurs, appelés nœuds du réseau et dont la liste est publique. Ce réseau permet de rendre anonyme l'origine de connexions TCP. Il peut ainsi servir à « anonymiser » la source d'une session de navigation Web ou de messagerie instantanée et est utilisé pour accéder aux marchés illicites du Dark Web.

Toutefois, une montée en puissance des capacités des groupes terroristes ouest-africains dans le domaine cyber ne peut être exclue à moyen et long terme, car quelques individus qualifiés peuvent suffire. En effet, les défaites territoriales de l'EI et leur volonté affichée de se greffer sur les conflits en Afrique subsaharienne[27] laissent craindre un afflux de moyens, de combattants et autres logisticiens sur le continent. S'il n'a été constaté jusqu'à présent aucune évolution majeure en ce sens, il convient d'adopter une démarche préventive et de s'assurer que les forces de l'ordre des États ouest-africains ont les capacités de détecter une utilisation de ces nouvelles technologies à des fins terroristes et d'y répondre.

Le risque de cyberterrorisme — attaque terroriste ayant pour cible les systèmes d'information de services publics ou d'entités privées — doit également faire l'objet d'une politique préventive. Quelques groupuscules de hackers ouest-africains se revendiquant djihadistes ont pris part à des opérations internationales, telles que l'attaque de défacement (ici le remplacement de la page d'accueil par un message de propagande) de différents sites Internet français après les attentats de janvier 2015[28]. Leur puissance de frappe semble limitée et le risque, mineur, mais il ne peut être totalement écarté au vu de la vulnérabilité des systèmes d'information dans les États de la sous-région.

Ces deux dernières problématiques restent cependant principalement prospectives et marginales comparées à l'enjeu critique et immédiat que représentent l'occupation de l'espace numérique et la diffusion d'information par les groupes terroristes actifs dans la sous-région.

2. Vers la conquête d'une souveraineté numérique

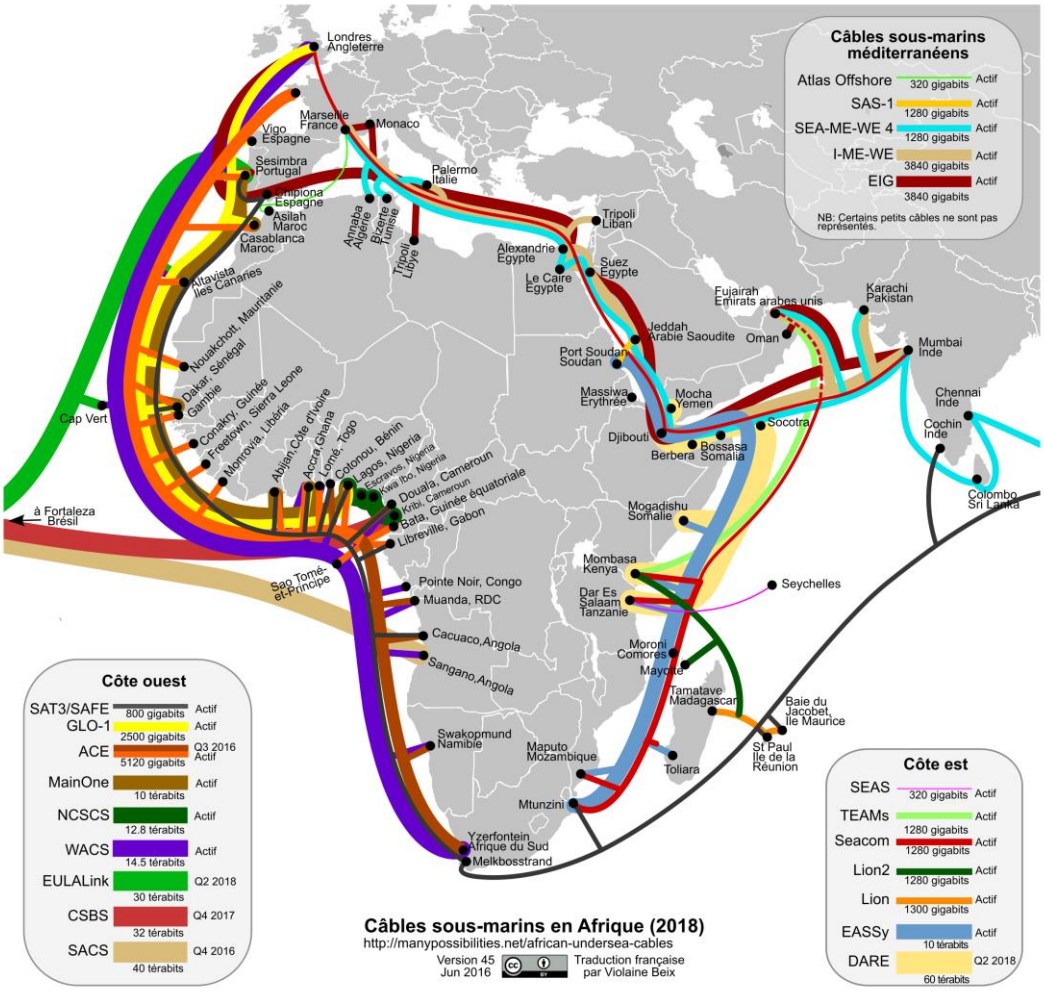
La conquête par les États d'Afrique de l'Ouest de leur souveraineté numérique ne se résume pas uniquement à des aspects de sécurité intérieure, mais doit faire l'objet d'une réflexion globale. Il n'existe pas de définition claire de la notion de souveraineté numérique, qui est communément utilisée pour désigner l'application de l'ensemble des principes de souveraineté aux technologies de l'information et de la communication[29]. Elle est protéiforme, extrêmement complexe et pourtant indispensable dans la réflexion actuelle des États sur le cyberespace.

27. Voir la série de vidéos d'allégeance publiées par diverses cellules en juin et juillet 2019, recensées sur @Jidhascope.

28. Plusieurs hackers ouest-africains auraient joué un rôle critique dans le collectif Anonghost. « Afrique de l'Ouest : le nouveau défi de la cybersécurité », *CEIS*, avril 2017.

29. Voir Jean-Gabriel Ganascia, Eric Germain et Claude Kirchner, « La souveraineté à l'ère du numérique », *CERNA*, octobre 2018.

Carte. Câbles sous-marins en Afrique (2018)



Source : *https://manypossibilities.net/african-undersea-cables/*

La souveraineté numérique d'un État se joue en effet dans les rapports de force entre Nations et sa capacité à garantir sa souveraineté économique et technologique, ainsi qu'un processus démocratique indépendant. Lors de son discours de mars 2018 sur l'intelligence artificielle, le président français Emmanuel Macron a, par exemple, défini la souveraineté nationale comme la capacité pour une nation de définir elle-même les normes auxquelles elle se soumet et non de se voir imposer ces règles de l'extérieur[30]. Il est bien sûr impossible pour une nation d'avoir un contrôle absolu sur son cyberespace sans remettre en cause le modèle de l'Internet ouvert, qui crée forcément des interdépendances. La souveraineté numérique peut cependant être regardée par les États comme un objectif relatif, placé au cœur de leur réflexion sur le cyberespace.

L'Afrique de l'Ouest se trouve actuellement dans une position défavorable pour peser dans ces nouveaux rapports de force. Un grand nombre de facteurs sont à prendre en compte pour évaluer la capacité d'un État à garantir sa souveraineté sur son espace numérique.

30. Discours du Président de la République sur l'intelligence artificielle, 28 mars 2018.

Deux facteurs primordiaux étant les infrastructures et les données. Parfois considérées comme les deux couches du cyberespace[31], elles servent de points de pression et de négociation dans les rapports avec les autres États et les acteurs privés comme les GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Le continent africain a longtemps été marginalisé en matière d'infrastructures numériques et beaucoup d'États enclavés de la sous-région sont toujours dépourvus de tout nœud, relai ou serveur important.

La construction de *data centers*[32] est également primordiale, puisqu'ils constituent un prérequis pour assurer l'indépendance technologique d'un État[33]. Les problématiques techniques telles que le climat et les faibles ressources énergétiques ont longtemps rendu impossible leur implantation sur le continent africain, qui accueillait en 2018 moins d'1 % de ces infrastructures. Si le secteur est en plein développement, les entreprises anglo-saxonnes du web ont donné la priorité à l'Afrique de l'Est et au Nigéria[34]. La côte ouest-africaine a pourtant un fort potentiel, les centres de données étant généralement placés au plus près des câbles et nœuds de relais. Mais la sous-région, à l'exception du Nigéria, de la Côte d'Ivoire et du Sénégal, manque de financements pour la construction de technopoles capables d'accueillir ces infrastructures[35].

2.1. Souveraineté économique et technologique : le risque de la captation de valeur

Les risques pour la souveraineté économique et technologique des États ouest-africains restent flous, mais on ne saurait les exclure. La politique commerciale agressive de la Chine sur le continent concerne également l'espace numérique d'Afrique de l'Ouest. Depuis plusieurs années, les entreprises de télécoms asiatiques, en premier lieu le groupe chinois Huawei, sont impliquées dans la quasi-totalité des projets de déploiement d'infrastructures réseau dans la sous-région. L'équipementier chinois propose des projets clé en main, financés grâce à des prêts concessionnels[36] par les banques chinoises aux gouvernements qui, souvent, ne disposent pas de ressources rapidement mobilisables pour financer des projets de cette ampleur[37].

31. Laurent Bloch, « Un nouvel espace stratégique : le cyberspace », 8 juin 2017.
32. Un *data center* ou centre de données, est une infrastructure composée d'un réseau d'ordinateurs et d'espaces de stockage. Cette infrastructure peut être utilisée par les entreprises pour organiser, traiter, stocker et entreposer de grandes quantités de données.
33. Charlotte Gonzales, Julien Dechanet, « L'essor du numérique en Afrique de l'Ouest, entre opportunités économiques et cybermenaces », CEIS, novembre 2015.
34. Données disponibles sur « Data Center Map », consulté le 25 août 2019.
35. « Data centers : Le Sénégal s'impose dans la gestion des données », *Jeune Afrique*, 12 juillet 2018.
36. Prêts dont le taux d'intérêt est inférieur aux taux du marché.
37. « Télécoms : la mauvaise fibre des groupes chinois en Afrique », *Jeune Afrique*, 7 juillet 2016.

Huawei a ainsi été chargé de la Dorsale transsaharienne de fibre optique, ligne de très haut débit Internet[38] qui reliera l'Algérie, le Nigéria, le Niger et le Tchad. L'entreprise a également équipé en réseaux de fibre optique le Sénégal, la Côte d'Ivoire ou encore la Guinée pour des centaines de millions d'euros, mettant à mal la traditionnelle coopération technique avec des groupes français[39].

Critiqués pour leur mauvaise exécution et l'absence de suivi[40], ces projets font partie d'une politique globale d'implantation de la Chine sur le marché africain qui passe également par des initiatives de formation d'ingénieurs et une communication visant directement le consommateur. Malgré les soupçons d'espionnage de son siège d'Addis-Abeba au profit du gouvernement chinois[41], l'Union africaine a signé avec Huawei en mai 2019 un protocole d'accord pour le renforcement de la coopération technique. Au sommet de la guerre commerciale qui oppose le géant chinois aux États-Unis, cette décision vient réaffirmer la position dominante de Huawei sur le marché africain.

Les GAFAM multiplient également les projets en Afrique subsaharienne pour capter les milliards d'utilisateurs potentiels que représente le continent. Les entreprises américaines ont cherché le moyen de garantir l'accès à leurs services à moindre coût. Facebook a par exemple lancé dès 2013 son projet *Internet.org*, depuis renommé *Free Basics*[42].

Ce partenariat mondial entre le réseau social et six entreprises de télécoms[43] vise à donner un accès gratuit à quelques services Internet présents sur la plateforme *Free Basics*, qui doivent respecter un format web simplifié. Dans le cadre de ce partenariat, les opérateurs téléphoniques ne facturent pas la bande passante à leurs clients pour l'accès à ces services. Il est d'ores et déjà accessible dans plusieurs États ouest-africains tels que le Sénégal, le Nigéria et le Ghana et sera bientôt disponible en Côte d'Ivoire. Par ailleurs, l'initiative *Facebook Zero*, distincte de *Free Basics*, donne un accès à une version texte du réseau social sans facturation de la bande passante par l'opérateur. Elle est présente au Bénin.

Ces stratégies dites de « *zero-rating* » semblent gagnantes pour tous les acteurs, puisqu'il a été estimé que la moitié des utilisateurs de *Free Basics* souscrivent à un abonnement Internet payant dans les 30 jours après le début de l'utilisation de la

38. « Dorsale Transsaharienne à fibre optique, 44 millions pour le tronçon nigérien », *La Tribune*, 14 décembre 2016.
39. « L'essor du numérique en Afrique de l'Ouest, entre opportunités économiques et cybermenaces », *CEIS*, novembre 2015.
40. « Télécoms : la mauvaise fibre des groupes chinois en Afrique », *Jeune Afrique*, 7 juillet 2016.
41. Enquête du *Monde* et du *Financial Times*, formellement contredite ensuite par Huawei et le gouvernement éthiopien. Voir « À Addis-Abeba, le siège de l'Union africaine espionné par Pékin », *Le Monde*, 26 janvier 2018.
42. Voir le site officiel d'Internet.org.
43. Samsung, Ericsson, MediaTek, Nokia, Opera Software et Qualcomm.

plateforme[44]. Ils deviennent ainsi pour une grande majorité des utilisateurs réguliers des réseaux sociaux du groupe Facebook.

En parallèle, les GAFAM financent de nombreux incubateurs de start-up, hackahtons[45] et centres de recherche sur le continent. Google vient par exemple d'ouvrir le premier centre de recherche africain sur l'intelligence artificielle (IA) à Accra, au Ghana[46]. L'intérêt pour les GAFAM est double : les données et le contrôle des innovations. Les pays en développement et sans régulation représentent un eldorado pour les données personnelles, qui serviront ensuite au ciblage publicitaire et au développement de l'IA. Ces initiatives permettent également d'être en première ligne dans le développement des innovations majeures sur le continent.

Les investissements de ces groupes, chinois ou américains, représentent de réelles opportunités économiques pour les États d'Afrique de l'Ouest et paraissent indispensables au développement rapide de leurs capacités numériques. Il existe cependant un risque important de captation de la valeur ajoutée par ces acteurs extérieurs si les gouvernements et universités ne développent pas d'initiatives propres[47], ce phénomène étant parfois qualifié de « *cybercolonialisation* »[48]. Le terme est largement utilisé dans la guerre commerciale entre les États-Unis et la Chine et est à prendre avec précaution. Il convient néanmoins d'éviter la création d'un écosystème numérique dont les ressources et profits bénéficieraient uniquement à des économies extérieures.
Sans des initiatives indépendantes et un réel effort des États de la sous-région dans le développement de leurs capacités technologiques, la relation avec les investisseurs restera déséquilibrée. Ce problème n'est évidemment pas spécifique à la sous-région et de nombreux États font face à la même difficulté d'avoir des pans entiers de leur vie numérique gérés par des groupes étrangers.

2.2. L'instrumentalisation d'Internet dans les processus électoraux

Les risques de désinformation en ligne et d'ingérence électorale sont universels, mais le contexte ouest-africain pourrait les rendre encore plus décisifs qu'ailleurs. Ces dernières années, avec l'augmentation massive de l'accès à l'Internet mobile, les pays africains se sont vus confrontés à l'apparition et la diffusion massive de fausses informations qui menacent les processus démocratiques. Un premier scandale africain a éclaté en 2018 avec la révélation du recours du président kenyan à la firme Cambridge Analytica.

---

44. Guillaume Champeau, « Les Free Basics de Facebook font les affaires des opérateurs partenaires », *Numerama*, 13 avril 2016.
45. Événement durant lequel des groupes de développeurs volontaires se réunissent pendant une période de temps donnée afin de travailler sur des projets de programmation informatique en mode collaboratif.
46. « GAFAM : l'Afrique face aux géants du web », *Jeune Afrique*, 16 août 2018.
47. « Intelligence artificielle en Afrique, le risque de captation de valeur existe selon Cédric Villani », *Le Monde*, 17 juin 2018.
48. « Intelligence artificielle : l'Afrique face aux géants du net », *Le Monde*, 17 décembre 2018.

L'entreprise aurait aidé le parti au pouvoir à mener des campagnes massives sur les réseaux sociaux lors des élections présidentielles de 2013 et 2017, en utilisant les données personnelles des utilisateurs[49].

Dans la sous-région ouest-africaine, l'élection présidentielle de février 2019 au Nigéria, particulièrement commentée sur les réseaux sociaux, a été un intéressant indicateur des risques de déstabilisation. La multiplication de fausses informations relayées par les différentes équipes de campagne et l'instrumentalisation de vidéos à des fins électorales ont été d'une ampleur sans précédent selon Reporters sans frontières[50]. À ces phénomènes s'ajoutent les potentielles tentatives de déstabilisation par des acteurs étrangers, particuliers ou étatiques. Les réseaux sociaux sont en train de devenir des outils performants d'influence ou d'ingérence pour des puissances extérieures, dont l'impact va être démultiplié par l'augmentation du nombre d'utilisateurs.

L'environnement ouest-africain rend la réponse à ces menaces particulièrement complexe. Les mesures prises par certains gouvernements ont souvent été radicales et tendent vers une restriction disproportionnée de la liberté d'expression. Le Tchad a par exemple pris des mesures successives de blocage des réseaux sociaux pendant plus d'un an[51] qui ont, selon l'ONG Internet sans frontières, généré un manque à gagner d'environ 18 millions d'euros pour le pays[52]. Une nouvelle loi donnant à l'autorité de régulation le pouvoir de prendre toute mesure de gestion du trafic qu'elle juge utile a également créé la controverse au Sénégal[53].
De nombreux cas de coupure totale d'Internet à la veille des élections ont également été constatés et le paysage médiatique de certains États empêche de trouver des sources d'information fiables. La reprise de ces fausses informations par certains médias et le faible taux d'éducation et de sensibilisation de la population amplifient le phénomène[54].

Dans ce contexte, il parait indispensable de protéger et développer la presse professionnelle et de préserver la neutralité du net. Les initiatives donnant accès à un nombre limité de services Internet comme *Free Basics* de Facebook ont d'ailleurs fait l'objet de vives critiques pour leur caractère attentatoire à cette neutralité et leur potentielle instrumentalisation dans des pays où les opérateurs téléphoniques sont parfois détenus par le pouvoir en place[55].

49. « Cambridge Analytica had a role in Kenya Election, too », *New York Times*, 20 mars 2018.
50. « Nigéria, RSF dénonce une campagne électorale polluée par la désinformation », *RSF*, 15 février 2019.
51. « Au Tchad, Idriss Déby fait lever le blocage des réseaux sociaux », *Le Monde*, 15 juillet 2019.
52. « Cybercriminalité, nouveau visage de la menace en Afrique », *La Tribune*, 13 avril 2019.
53. « Sénégal, vers la censure des réseaux sociaux ? », *TV5 Monde*, 1er décembre 2018.
54. « Cybercriminalité, nouveau visage de la menace en Afrique », *La Tribune*, 13 avril 2019.
55. « Facebook plan to wire Africa is a dictator's dream », *Foreign Policy*, 27 octobre 2016.

Là encore, la solution réside en partie dans l'éducation de la population par des campagnes de prévention, ainsi que dans le développement d'outils de vérification par des organismes indépendants, comme cela a été observé au Nigéria en 2019[56].

3. La nécessaire harmonisation des réponses

L'absence de frontières dans le cyberespace rend les réponses purement nationales insuffisantes et, si l'adoption par chaque État d'une stratégie concernant le cyberespace englobant les divers aspects susmentionnés est un préalable, il est indispensable de chercher une vision commune pour la sous-région. Ces réponses visant à garantir un Internet sûr doivent aller au-delà d'une approche purement sécuritaire et s'attacher à la recherche d'un équilibre qui préserve les libertés individuelles et les opportunités économiques liées à l'utilisation des nouvelles technologies.

3.1. Vers un cadre juridique commun ?

Pour pouvoir coopérer, les pays de la sous-région ont besoin d'un cadre juridique commun, a minima sur la lutte contre la cybercriminalité et si possible également sur la protection des données personnelles. S'il n'existe pas de convention onusienne en matière de lutte contre la cybercriminalité, les États ouest-africains disposent de plusieurs instruments internationaux. La Convention du Conseil de l'Europe sur la cybercriminalité, aussi appelée Convention de Budapest[57], est entrée en vigueur en 2004 et est ouverte aux États non membres. Malgré l'absence de consensus international[58], elle est considérée par les États occidentaux comme le traité de référence pour la coopération internationale en matière de cybercriminalité et 63 États l'ont ratifiée à ce jour.

L'Union africaine a également adopté en 2014 une convention sur la cybersécurité et la protection des données à caractère personnel[59] – dite Convention de Malabo – qui invite les États à adopter des mesures législatives et réglementaires. Ce traité, visant à apporter une réponse régionale à ces menaces, a cependant connu un échec, puisqu'en 2019 seulement cinq États l'ont ratifié (le Ghana, la Guinée-Bissau, l'Île Maurice, la Namibie et le Sénégal). Les États d'Afrique de l'Ouest se sont jusqu'alors très peu emparés de ces instruments, qui pourraient pourtant faciliter leur coopération en assurant une base juridique commune. Le Sénégal et le Ghana ont récemment ratifié la Convention de Budapest et se posent ainsi en leaders espérant déclencher un mouvement vers la ratification dans la sous-région.

56. Voir le projet collaboratif Crosscheck Nigeria.
57. Voir le texte officiel de la Convention sur la cybercriminalité du Conseil de l'Europe.
58. La Russie et la Chine s'opposent fermement au texte et œuvrent pour la négociation d'un nouveau traité au sein des Nations unies.
59. Voir le texte officiel de la Convention sur la cybersécurité et la protection des données à caractère personnel de l'Union africaine.

Malgré cette absence de socle commun, la sous-région a connu ces dernières années l'adoption de nombreux textes législatifs dans ce domaine. L'adoption en 2011 d'une directive portant lutte contre la cybercriminalité par la Communauté économique des États d'Afrique de l'Ouest (CEDEAO) a permis de définir les principales infractions et d'appeler les États à légiférer[60]. Si une majorité d'États ont déjà entériné des lois contre la cybercriminalité, les pays du G5 Sahel[61] accusent un sérieux retard au niveau des législations. Des textes sont actuellement en discussion au Burkina Faso et au Niger, tandis qu'il n'existe à ce jour aucune législation spécifique au Tchad et en Mauritanie[62]. Le cadre législatif en matière de protection des données personnelles est également disparate.

Outre ce paysage juridique fragmenté, il existe d'importantes différences dans la mise en œuvre de la lutte contre la cybercriminalité et des moyens qui lui sont attribués. Alors que le Sénégal, la Côte d'Ivoire et les pays anglophones se sont dotés de centres d'alerte et de réaction aux attaques informatiques (CERT)[63] et d'unités de police spécialisées, beaucoup de pays n'ont aujourd'hui aucun mécanisme de réponse spécifique malgré ce qui est prévu par les textes. L'adoption de mesures législatives et de stratégies nationales de cybersécurité par l'ensemble des pays de la sous-région, ainsi que la mise en place de structures dédiées, est donc le premier pas pour répondre aux menaces actuelles.

Au vu de la situation sécuritaire dans les pays de la bande sahélienne, la réponse est d'autant plus urgente et elle ne doit pas être négligée dans les tentatives de stabilisation de la zone.

3.2. Une aide internationale plus cohérente

L'instabilité dans la bande sahélienne et sa propagation à d'autres régions de l'Afrique de l'Ouest est une préoccupation majeure pour de nombreux États et organismes internationaux. La sous-région bénéficie ainsi d'une aide internationale importante, allouée en grande partie aux interventions militaires et au développement.

60. Voir le texte officiel de la Directive C /DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDAEO.

61. Le G5 Sahel ou « G5S » est un cadre institutionnel de coordination et de suivi de la coopération régionale en matière de politiques de développement et de sécurité, créé en février 2014 par cinq États du Sahel : Mauritanie, Mali, Burkina Faso, Niger et Tchad.

62. « Cybercrime Legislation Worldwide », *UNCTAD*, consulté le 25 août 2019.

63. Un *computer emergency response team* ou *computer security incident response team* est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Le coût des opérations militaires comme l'opération Barkhane, dont le budget annuel est supérieur à 650 millions EUR[64], a cependant encouragé les bailleurs à adopter une approche globale qui se concentre sur le renforcement des institutions régaliennes[65].

Un certain nombre de projets de coopération policière et judiciaire axés sur le cyber ont vu le jour. La plupart de ces initiatives sont bilatérales. Les États-Unis se sont par exemple beaucoup impliqués au Nigéria et au Ghana, tandis que la France a soutenu la création de la division de cybersécurité de la Police nationale du Sénégal[66]. Le Conseil de l'Europe et l'Office des Nations unies contre la drogue et le crime (ONUDC) ont également des projets visant à appuyer les autorités policières et judiciaires pour lutter contre la cybercriminalité dans la sous-région. Néanmoins, la multiplication des acteurs et leur manque de coordination causent des redondances dans les formations proposées et une réelle fragmentation de l'aide. Les contraintes généralement imposées par les bailleurs (des budgets limités sur des périodes très courtes) les empêchent également de proposer un support global. Ainsi, de nombreux bénéficiaires regrettent un système de formations courtes sans véritable suivi sur le long terme ni fourniture d'équipements adaptés[67].

Dans le domaine du cyber, il ne s'agit pas seulement de renforcer les institutions régaliennes en charge, mais aussi parfois de soutenir la création de tout le dispositif national de cybersécurité. Cela demande de concevoir des projets qui s'intéressent à toutes les étapes du processus, c'est-à-dire aux aspects législatifs, institutionnels et opérationnels. Les organisations et États menant des projets de coopération technique dans le domaine doivent également s'assurer que la lutte contre la cybercriminalité et l'utilisation d'Internet à des fins terroristes s'inscrit dans une réflexion globale sur la cybersécurité et la cyberdéfense du pays.

La récente inauguration à Dakar de l'École nationale à vocation régionale (ENVR) de cybersécurité laisse espérer des changements. Les ENVR sont une initiative de la France visant à renforcer la sécurité globale des pays africains, il en existe aujourd'hui quinze sur le continent[68]. Cette école de cybersécurité, fondée sur un partenariat interministériel franco-sénégalais, vise à dispenser des formations techniques, mais également des formations stratégiques aux cadres des administrations concernées par le cyber[69]. Elle ambitionne également de devenir un pôle pour la coopération dans la sous-région.

---

64. Serge Michailof, « Sahel : Face à l'insécurité, l'aide publique au développement ne peut pas se contenter de slogans », *IRIS*, décembre 2017.
65. Voir par exemple pour la France, Rapport d'information du Sénat, « Sahel : repenser l'aide publique au développement », 29 juin 2016.
66. « Sénégal : la Police emploie les grands moyens pour la cybersécurité », *Jeune Afrique*, 20 juin 2017.
67. Entretiens menés à Dakar en décembre 2018.
68. Voir la page consacrée du site du ministère de l'Europe et des Affaires étrangères français.
69. « Sénégal : inauguration de l'école nationale de cybersécurité à vocation régionale de Dakar », *France Diplomatie*, novembre 2018.

Enfin, il demeure indispensable d'intégrer davantage la question des libertés individuelles aux différents projets mis en œuvre. Alors que cet enjeu a trouvé sa place dans la coopération policière et judiciaire sur de nombreuses thématiques, il reste rarement abordé lorsqu'il s'agit de cybersécurité. L'impact à moyen et long termes de projets proposant une vision purement sécuritaire sans sensibilisation sur la liberté d'expression et la protection des données personnelles pourrait être dommageable et engendrer des politiques attentatoires aux libertés, visant au contrôle absolu des nouveaux moyens de communication.

3.3. La coopération internationale comme pierre angulaire

Les problématiques de cybersécurité, et en particulier la cybercriminalité, sont le plus souvent transfrontalières. Dans le contexte ouest-africain, il ne peut y'avoir de réponse efficace sans une coopération interagences et internationale forte et rapide, notamment au niveau opérationnel. Une fois les États dotés de mesures législatives harmonisées et de structures dédiées, il est important de penser les différents réseaux et structures pouvant renforcer la coopération au niveau de la sous-région. Le Centre européen de lutte contre la cybercriminalité (EC3), qui officie sous l'égide d'Europol, pourrait être un modèle intéressant. Il permet une coopération directe et rapide entre les polices des différents États membres et joue aujourd'hui un rôle central dans les enquêtes transnationales. Le mécanisme de coopération policière Afripol[70], lancé en 2015 par l'Union africaine[71], serait en principe en mesure d'accueillir une structure semblable. Malgré les bureaux de liaison ouverts récemment dans 40 pays, il parait cependant assez peu probable que les États de tout le continent acceptent de coopérer étroitement sur ces problématiques.

À l'heure actuelle, la coopération informelle par le biais de points focaux dans les plateformes de lutte contre la cybercriminalité semble l'option la plus réaliste et la plus efficace.

Cette coopération existe déjà de manière régulière avec des États occidentaux et de manière ponctuelle entre certains États de la sous-région, les plateformes de lutte contre la cybercriminalité du Sénégal et de la Côte d'Ivoire mettant notamment leurs compétences et équipements au service d'enquêtes transnationales avec d'autres pays ouest-africains[72]. Cette coopération directe a fait ses preuves par exemple lors de l'enquête qui a suivi les attentats terroristes de 2017 au Burkina Faso.

70. Afripol est un mécanisme de coopération policière basé à Alger qui vise à favoriser l'échange de renseignements entre les polices nationales des États africains et à faire émerger une stratégie harmonisée de lutte contre la criminalité organisée. Voir le texte officiel des Statuts d'Afripol.

71. « Police : Afripol ouvre des bureaux de liaison dans 40 pays », *Le Point*, 16 octobre 2018.

72. Voir, par exemple, les rapports d'activité de la DITT de la Police nationale de Côte d'Ivoire.

Grâce au soutien de la Police nationale de Côte d'Ivoire pour l'analyse des preuves numériques et notamment des communications passées par les attaquants, les forces de l'ordre burkinabé ont pu démanteler le réseau et découvrir des liens avec d'autres attaques[73].

La coopération dans la sous-région ne devrait toutefois pas se limiter aux domaines policier et judiciaire. Il est important d'utiliser les différents forums existants pour définir une vision commune du cyberespace dans la sous-région. L'adoption de la Convention de Malabo et l'accent mis sur le cyber lors des dernières éditions du Forum international de Dakar sur la paix et la sécurité en Afrique montrent une réelle volonté politique de certains États. Le Sénégal, la Côte d'Ivoire ou le Ghana ont déjà pris conscience des enjeux majeurs du cyberespace et ont mis en place des stratégies nationales ambitieuses sur le numérique. Il existe cependant un fort attachement à la souveraineté nationale en Afrique de l'Ouest et une certaine réticence à accepter des normes régionales contraignantes, comme en témoigne le faible nombre de ratifications de la Convention de Malabo. L'exemple européen montre pourtant qu'il faudra surmonter cette réticence pour que la sous-région puisse être audible et défendre ses intérêts dans la géopolitique du cyberespace.

Conclusion

Il est aujourd'hui essentiel que les États ouest-africains assurent la sécurité de leurs citoyens en ligne et exercent leurs fonctions régaliennes sur le cyberespace. La cybercriminalité est un phénomène complexe et protéiforme et est un enjeu crucial pour le présent et le futur de la sous-région. Les causes de ces évolutions sont multiples : croissance exponentielle de la couverture Internet mobile, adoption massive de technologies telles que le paiement mobile, manque d'éducation sur les risques liés à l'utilisation d'Internet et de programmes de prévention. Le développement des formations universitaires en informatique conjugué à une insuffisance de débouchés professionnels pour les jeunes ingénieurs a également contribué à l'augmentation du nombre de cybercriminels[74]. Au-delà du préjudice direct engendré par ce phénomène, la perte d'opportunités liée à l'absence de confiance dans les économies digitales de certains pays d'Afrique de l'Ouest est particulièrement inquiétante. Difficilement chiffrable, ce manque à gagner pourrait à long terme et de manière insidieuse mettre en danger les transitions numériques entamées par ces États.

De plus, les menaces cyber sont intrinsèquement liées aux autres défis auxquels la sous-région doit faire face. Les premiers signes de radicalisation en ligne et l'adaptation des stratégies de propagande des groupes terroristes ouest-africains à l'ère des réseaux sociaux attestent de cette évolution.

---

73. Entretien à Abidjan, Côte d'Ivoire, février 2019.

74. En Côte d'Ivoire on observe une hausse des plaintes durant les vacances scolaires, ce qui laisse supposer qu'une grande part des cybercriminels sont encore étudiants, voir le rapport d'activité DITT pour l'année 2016.

Dans le contexte sécuritaire actuel, le développement de réelles capacités d'enquête sur les supports numériques doit donc être une priorité absolue dans tous les États de la sous-région. L'absence de l'État dans une partie des territoires est l'une des causes principales d'instabilité dans les pays du Sahel. Un manque d'investissement dans le cyberespace pourrait créer une nouvelle zone de non-droit aux effets étendus et diffus.

La réponse sécuritaire doit également être intégrée dans une réflexion plus large sur la souveraineté numérique nationale. Le développement extrêmement rapide de l'écosystème numérique et les faibles investissements publics rendent le risque de captation de valeur par des acteurs extérieurs plus fort qu'ailleurs. Pour éviter une dépendance totale envers ces acteurs extérieurs, il serait également nécessaire de privilégier le financement de projets sur les ressources propres de l'État[75] ou des partenariats à long terme permettant à l'État bénéficiaire de s'investir progressivement dans la gouvernance des infrastructures ou des centres de recherche. L'adoption de véritables stratégies nationales de cybersécurité et de cyberdéfense, ainsi qu'une réflexion sur les investissements étrangers, est une première étape essentielle pour identifier et limiter les risques. La question complexe de l'équilibre ténu entre la lutte contre la désinformation et la préservation de la liberté d'expression doit être incluse dans cette réflexion en amont, afin de préserver les processus électoraux et d'éviter l'accumulation de mesures de circonstance.

De nombreux éléments de réponse sont actuellement mis en œuvre dans la sous-région. Devant le caractère complexe et transfrontalier des menaces, il est cependant primordial de renforcer la coopération régionale, au niveau opérationnel comme au niveau politique.

* * *

L'auteure

Coline Mechinaud, diplômée d'un Master en Administration internationale de l'Université Paris-I Panthéon Sorbonne, est spécialisée dans les questions liées à la coopération internationale et aux organisations multilatérales. Elle a travaillé deux ans comme consultante pour l'Office des Nations unies contre la drogue et le crime (ONUDC) sur des thématiques telles que l'anti-blanchiment d'argent et la lutte contre la cybercriminalité.

75. Le Rwanda est souvent cité comme modèle à suivre, avec des infrastructures financées par les ressources de l'État et des partenariats longs. Voir « Télécoms : la mauvaise fibre des groupes chinois en Afrique », *Jeune Afrique*, 7 juillet 2016.