



HONNEUR
& FIDÉLITÉ
HONOR
& LOYALTY



INTELLIGENCE ÉCONOMIQUE ET CYBER CRIMINALITÉ.

Impact sur l'activité économique en Afrique Centrale

Analyse de

Dr Christian POUT, Ministre Plénipotentiaire,
Président du Think Tank CEIDES,
Directeur du Séminaire de Géopolitique Africaine à l'Institut Catholique de Paris

Publiée dans le Bulletin "Honneur et Fidélité" des Forces de Défense Camerounaises de
décembre 2020, aux pages 50-53.

Janvier 2021

Les experts sont de plus en plus unanimes pour affirmer que les technologies de l'information et de la communication (TIC) occupent une place de plus en plus incontournable dans les sociétés du XXIème siècle. La transformation numérique induite par les TIC a ainsi contribué à la croissance économique, à la création d'emplois directs et indirects, au développement des ressources humaines et au renforcement des institutions. L'Afrique est le continent dont la population connaît la plus forte croissance démographique (soit un taux de croissance annuel de 2,5% contre un taux de 1,12% au niveau mondial), avec une forte proportion de population jeune plus encline à l'utilisation des NTIC.

1. Perspectives de l'économie numérique en Afrique centrale

Selon le rapport « La consommation en Afrique - Le marché du XXIe siècle » du cabinet Deloitte, plus de 200 millions d'Africains, soit plus de 20 % de la population totale de jeunes, sont âgés de 15 ans à 24 ans. Il précise que ce chiffre devrait passer à 321 millions d'ici à 2030 et que les jeunes Africains, soit une grande partie de la classe moyenne émergente, aspireront à un plus grand choix de produits et de services, ainsi qu'à une plus grande connectivité. L'Afrique devrait devenir le deuxième marché le plus important pour les investissements des sociétés européennes des biens de consommation. Cette tendance est davantage importante dans le domaine des TIC. En effet, l'Afrique sub-saharienne enregistre le taux le plus élevé de croissance des télécommunications mobiles dans le monde, avec un taux annuel composé (CAGR) de 6,1%, selon le rapport 2017 de GSMA sur l'économie du secteur mobile en Afrique Sub-Saharienne, et cette tendance devrait se poursuivre sur plusieurs années encore. Ce développement des TIC est de nature à contribuer à l'atteinte des Objectifs du Développement Durable (ODD), ainsi qu'affirme Houlin Zhao, Secrétaire Général de l'Union Internationale des Télécommunications (UIT) : « Les TIC offrent des possibilités exceptionnelles pour accélérer les progrès en matière de réalisation des ODD et améliorer la vie des personnes de façon radicale».

Concernant l'Afrique Centrale, la plupart des pays se trouvent affectés par l'effondrement des cours des principaux produits de base, dont le pétrole, et par le ralentissement de l'activité économique en réponse à la pandémie du COVID19 ; et font face à des déséquilibres macroéconomiques importants marqués par un fléchissement de la croissance économique. Lors de la 33eme session du Comité Intergouvernemental d'Experts (CIE) d'Afrique Centrale, tenue en 2017 à Douala (Cameroun), à travers le

Consensus de Douala, un appel à l'action a été lancé en direction des acteurs majeurs des secteurs public et privé, pour passer du cercle vicieux de l'exportation des matières premières non transformées au cercle vertueux de l'ajout de la valeur aux ressources naturelles, grâce à la diversification et l'industrialisation de leurs économies. La transformation numérique est un pilier clé de cette stratégie de diversification économique et d'industrialisation. En prenant l'exemple du commerce électronique, qui s'appuie sur la chaîne logistique pour son développement, il apparaît que l'intégration sous régionale ou encore la zone de libre-échange continentale africaine (ZLECAf) sont des cadres favorables à l'essor de l'économie numérique.

Les défis à relever sont nombreux. On peut citer l'extension de l'interconnexion sous régionale à toutes les populations. En effet, les capacités en infrastructures large bande à fibre optique sont encore faibles, l'ossature devant relier les pays entre eux reste encore à mettre en place, et les prix des communications électroniques, en comparaison avec les autres régions du monde et le niveau de revenu, sont très élevés. Une autre priorité porte sur l'amélioration permanente de la qualité de service et d'expérience du consommateur des communications électroniques afin de garantir la disponibilité des services 24 heures sur 24 et 7 jours sur 7, dans des environnements où le réseau à fibre optique fait parfois l'objet de coupure alors que sa redondance n'est pas toujours assurée, ou même le réseau électrique est peu stable, tout ceci sans occulter les questions de qualité propre de la communication. Le cadre légal et réglementaire est défini par la CEEAC dans des lois types pour harmoniser les politiques et garantir leur cohérence. Huit lois types dans le domaine du numérique sont en vigueur et sont ainsi libellées :

- Loi type portant cadre Juridique et Institutionnel général du secteur de communications électroniques - Brazzaville novembre 2016
- Loi type relative aux régimes d'accès et aux activités de communications électroniques -Brazzaville, novembre 2016 ;
- Loi type relative au service universel et les mécanismes de son financement - Brazzaville, novembre 2016 ;
- Loi type relative aux fréquences radioélectriques et aux ressources en numérotation - Brazzaville, novembre 2016 ;
- Loi type relative à l'interconnexion - Brazzaville, novembre 2016 ;
- Loi-type relative aux transactions électroniques ;
- Loi-type relative à la protection des données à caractère personnel ;

- Loi-type portant sur la lutte contre la cybercriminalité dans les Etats Membres de la CEEAC/CEMAC.

Cependant, malgré l'existence de cette armature légale et réglementaire le niveau de transposition de ces lois types dans les législations nationales des onze Etats membres de la CEEAC reste faible. Ceci étant la conséquence du non démarrage de la deuxième phase pour l'accompagnement et le suivi de leur transcription dans les lois nationales. Il faut également mettre en relief que tout en sachant que l'économie numérique repose de plus en plus sur les données (Big data, IA, etc.), la plupart des pays ne disposent pas de lois sur la protection des données à caractère personnel. En plus du respect de la loi, il apparaît majeur de régler ou tout au moins annihiler les effets de la cybercriminalité pour garantir la vitalité de notre économie et la sécurité des concitoyens et des partenaires économiques et financiers.

2. L'impact de la cybercriminalité sur l'économie en Afrique centrale

Placer le débat numérique au cœur de la pensée stratégique est un impératif catégorique dans ce 21^{ème} siècle pour toute nation ou communauté économique régionale (CER) soucieuse de la sécurité de ses systèmes et réseaux d'informations ou plus simplement de sa sécurité intérieure et surtout de son économie. En effet, comme démontré la numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. L'espionnage, la propagande, le sabotage, l'exploitation excessive de données personnelles et pour ce qui nous interpelle la cybercriminalité, menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel, composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il en va de même pour les Etats. Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de «

l'intelligence des risques » elle-même composante de l'intelligence économique. », selon l'expert Bernard Besson.

Dans le cyberspace africain, de nouveaux crimes, risques, infractions et menaces sont apparus parmi lesquels : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme. Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; elles peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour le délinquant. La cybercriminalité est entendue comme l'ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet. Elle se traduit par des attaques informatiques et de vols de données, menées en grande partie par des réseaux criminels locaux. Elles ciblent principalement les banques, les agences gouvernementales et les entreprises de taille moyenne, mais elles visent également les PME dont les opérations commerciales dépendent d'internet. Ces dernières sont les cibles de piratage de grande envergure alors qu'elles ont peu de moyens (techniques ou financiers) pour y faire face. A titre illustratif, selon l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) du Cameroun, 12 800 cyberattaques ont été enregistrées en 2017 et 49 millions de cyberattaques ont été neutralisées par Kaspersky en Afrique au premier trimestre 2014. Ces attaques ont une incidence désastreuse sur l'économie. A cet effet, selon une enquête réalisée par une entreprise de conseil en cybersécurité (SERIANU), la criminalité informatique a fait perdre à l'Afrique près de 3,5 milliards de dollars en 2017. Un site spécialisé nous informe en ce sens que l'Afrique enregistre des centaines de millions de cyberattaques par an. Les banques et les administrations sont les plus ciblées par les hackers ; L'Afrique du Sud, le Nigéria, le Kenya payent un lourd tribut au fléau. Selon une estimation - de la même source - généralement acceptée, la cybercriminalité coûte à l'économie mondiale la somme de US\$ 500 milliards, soit plus que le Produit Intérieur Brut de l'Afrique du Sud (350.6 milliards de dollars) et un peu moins que celui du Nigeria (521.8 milliards de dollars), la première économie du continent qui perd en moyenne US\$ 500 millions - environ 300 milliards de Francs CFA du fait des cyberattaques.

3. L'importance des Forces de défense et de sécurité dans la lutte contre la cybercriminalité

En définitive, la plupart des pays de la CEEAC ont donné une place de choix aux TIC et à l'économie numérique dans leur vision et leur politique de développement à long et moyen terme. L'économie numérique paraît en conséquence être un catalyseur du développement sur lequel l'Afrique Centrale devrait s'appuyer pour sa diversification économique et son industrialisation. Dans cette mouvance, bien que la transformation numérique soit une question transversale qui concerne tous acteurs de la société et de l'économie, le rôle de l'Etat, par le truchement de ses organes en charge des questions de défense et de sécurité, reste central.

En effet, si internet est un espace de liberté, cette liberté ne saurait être absolue, dès lors que cet espace est utilisé pour porter atteinte à la sécurité de l'État ou de citoyens. Les attaques menées dans le cyberspace font subir aux particuliers et aux entreprises des dommages considérables. Elles peuvent aller jusqu'à porter atteinte au fonctionnement voire à l'existence des institutions ou des opérateurs essentiels à la vie de la Nation. Elles constituent de ce fait des atteintes inacceptables à la sécurité. Face au développement de la cybercriminalité, les forces de défense et de sécurité doivent inscrire leur action dans une stratégie ambitieuse de lutte contre les cybermenaces pour se protéger et protéger l'ensemble de la communauté. C'est pourquoi il est essentiel qu'une vision stratégique du rôle, des missions et de l'action de l'Etat soit déclinée en cohérence avec l'action communautaire. La création d'un organe communautaire en charge de la lutte contre les cybermenaces serait une première réponse à l'affirmation d'une visibilité plus forte de l'action des gouvernements en ce domaine.

Le Centre africain d'Etudes Internationales, Diplomatiques, Économiques et Stratégiques (CEIDES) est un laboratoire d'idées qui cumule plus d'une dizaine d'années d'expérience dont six d'existence officielle sous la forme d'une association indépendante, à caractère scientifique et à but non lucratif.

Le CEIDES a vocation à contribuer à la paix et à la prospérité du continent. Il s'engage ainsi à travers la stratégie, la recherche, le conseil, l'influence et la formation dans le cadre du continuum des 3D Développement/Diplomatie/Défense.

Il compte 4 Clubs actifs qui rassemblent des décideurs, chercheurs et partenaires à différentes échelles.

L'intelligence des situations et des contextes, sans enfermement systémique, par recours à la rigueur méthodologique des sciences sociales, la capacité à mettre en place des espaces ouverts, transdisciplinaires et multiacteurs de dialogue structuré et en partager le fruit par des mécanismes de lobbying et plaidoyer sont notre cœur de métier.



ceides
Centre africain d'Etudes Internationales
Diplomatiques Economiques et Stratégiques

B.P. 35147 Bastos-Yaoundé/Cameroun

Tél : (+237) 243 105 872

www.ceides.org Email : infos@ceides.org



Think tank Ceides