No. 64 MAI- JUIN 2020

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

cio mag .com

DOSSIER SPÉCIAL

LES GRANDS ENJEUX DE LA CYBERSÉCURITÉ EN AFRIQUE

CORONAVIRUS

L'innovation comme réponse à la crise

Quelles mesures gouvernementales pour limiter l'impact ?

Ndèye Tické Ndiaye Diop
MINISTRE DE L'ECONOMIE NUMÉRIQUE ET DES TÉLÉCOMS DU SÉNÉGAL

Yacine Oualid
MINISTRE DÉLÉGUÉ CHARGÉ DES START-UP DE L'ALGÉRIE

ZONE CFA AVION : 3000 FCFA - ZONE CFA SURFACE : 2000 FCFA - MAR : 55DH - FRANCE MÉTRO : 4,50€ - ESP : 4,50€ - CANADA : 8$ CAD


OLYMPIC®
BANKING SYSTEM
Ready for your
digital transformation
8%
14%
78%
The leading banking software by
30 eRI®
YEARS OF EXCELLENCE
www.olympicbankingsystem.com
Geneva London Lugano Luxembourg Paris Singapore Zurich

Édito

Mohamadou DIALLO
FONDATEUR ET DIRECTEUR GÉNÉRAL DECIO MAG

Face au Covid-19, l'Afrique a déjoué tous les pronostics. Qu'en sera-t-il à présent de la gestion de l'après-crise ? Eléments de réponses lors des prochains E-Conf Challenges.

« L'Afrique doit se préparer au pire. Elle doit s'y préparer dès aujourd'hui », prédisait, dès le 19 mars, l'Ethiopien Tedros Adhanom Ghebreyesus, Directeur général de l'Organisation mondiale de la Santé (OMS). Certes, son excès de catastrophisme a fait resurgir les vieux démons des tenants de l'afro-pessimisme, que l'on pensait avoir dépassés après des années d'une croissance soutenue. Mais, son propos a néanmoins incité les Africains au dépassement de soi. En effet, au moment où les grandes puissances subissaient les effets désastreux de la pandémie, l'Afrique se mettait en ordre de bataille pour anticiper, dès la première heure, l'arrivée du Coronavirus. Aujourd'hui, le continent déplore le décès de 2 126 personnes, soit moins de 1% du bilan mondial de l'épidémie estimé à 276 000 morts, le 9 mai 2020.

Aguerri par des décennies de crises sanitaires, l'Afrique a démontré sa capacité d'adaptation et de résilience, malgré la fragilité des systèmes de santé. Ironie du sort, pour la première fois de l'histoire, c'est l'Afrique qui est en pole position. Les raisons en sont multiples. Elles s'expliquent par l'accumulation du savoir-faire africain dans la gestion des crises précédentes, comme ce fut le cas pour le paludisme et plus récemment pour Ebola. Et du fait de la jeunesse de sa population.

Au-delà de ces avantages inhérents à l'Afrique, ce qui a primé, c'est d'avoir anticipé la mise en place des gestes barrières. La faible intégration du continent africain à la mondialisation économique a également permis de juguler l'épidémie. Ce phénomène est subitement apparu comme crucial, si bien que l'on envisage à présent de relocaliser des industries.

Rien ne sera plus comme avant

La majorité des 3,4 milliards de terriens (43% de la population mondiale), qui a vécu de façon inédite le confinement, pense que rien ne sera plus jamais comme avant. Au moment où s'amorce le déconfinement, un certain nombre de questions existentielles se posent à l'humanité. Si la gestion de la crise a été bien maitrisée, qu'en sera-t-il de la stratégie de sortie ? Les enjeux futurs se cristallisent autour de cette équation. D'ores et déjà, l'on parle de l'avènement d'un nouvel ordre mondial. Et du risque de déstabilisation d'une gouvernance économique mondialisée à outrance depuis plusieurs décennies. Entre fantasme et réalité, la mondialisation a fini par montrer ses limites. Les délocalisations et autres externalisations ont jusqu'alors été théorisées pour thésauriser et faire basculer la concurrence fiscale entre Etats. Les pays occidentaux se préparent à une vague de relocalisation des industries considérées comme stratégiques, voire vitales. Qu'en sera-t-il en Afrique, où la balance commerciale enregistre un déficit chronique dans bien des secteurs relevant de sa souveraineté ?

E-Conf Challenges

Ces questionnements sont à l'origine de la série d'E-Conf Challenge, que nous avons organisée pour approfondir la réflexion avec les décideurs du continent africain. Lors de la seconde édition, Lacina KONE, CEO de Smart Africa, a affirmé qu'il s'agissait plus que jamais de s'adapter, si l'on ne voulait pas disparaitre.

Après la série d'E-conf Challenge dédiée à la gestion de la crise sanitaire, et à l'impact du Coronavirus sur la digitalisation des entreprises et des administrations africaines,CIO Mag entame une seconde série de conférences.

A l'ordre du jour, les enjeux de l'après-crise et les réponses à apporter aux questionnements :

Quels sont les grands enseignements de cette crise pour l'Afrique ? Comment le continent doit-il aborder son avenir ? De quelle manière peut-on optimiser la connexion entre le système de santé et le numérique ? Comment intégrer aux projets de R&D le contingent d'innovateurs, qui a fourni de manière désintéressée des solutions durant la crise ?

Autant de questions qui nous interpellent avec beaucoup d'acuité.

CIO Mag vous donne rendez-vous prochainement pour élaborer des éléments de réponses.

SOMMAIRE

N°64 MAI - JUIN 2020

L'AFRIQUE EN CHIFFRES 06

ILS ET ELLES ONT DIT ... 07

E-CONF CHALLENGE

Les E-Conf Challenge pour mettre en lumière les innovations anti-Covid-19 en Afrique 08

SÉNÉGAL
« Le digital permet d'assurer la continuité des activités économiques » 09

ALGERIE
« Transformer le pays en Start-up nation, c'est notre ambition » 12

DOSSIER CYBER SÉCURITÉ

CYBERSÉCURITÉ
Les actes de cybercriminalité ont-ils atteint leur pic en Afrique ? 14

« La cybersécurité conditionne l'efficacité de la gouvernance numérique » 18

AFRIQUE
Des cadres légaux adaptés aux menaces cybersécuritaires ? 22

COVID-19
Les cybers risques, l'autre guerre de la crise sanitaire 24

SENEGAL
La coopération franco-sénégalaise à l'origine de l'école de formation des élites africaines 26

BÉNIN
Epitech sort sa première promotion d'experts en informatique en 2021 28

FORMATION
Pourquoi envisager une carrière dans la cybersécurité ? 30

BÉNIN
Face au Covid-19, l'ANSSI plus que jamais d'attaque 32

AFRIQUE DU SUD
Un niveau de risque de cyberattaques inquiétant 34

AFRIQUE
« La cybersécurité n'est plus une option » 37

CÔTE D'IVOIRE
La fraude au portefeuille électronique, une cyber-escroquerie redoutable 39

CORONAVIRUS
Attention au phishing 41

PUBLIREPORTAGE

Michel Van Den Berghe,
CEO Orange Cyberdéfense
« Intégrer plus en amont les critères de cybersécurité » 45

Francis Meston,
Directeur Atos Afrique, Moyen Orient
« La menace cyber matérialise la guerre économique dans laquelle nous sommes entrés » 48

Adnane Ben Halima, Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei Northern Africa
« La cybersécurité est l'une des principales priorités de Huawei » 51

PAROLES D'EXPERTS

MAROC
Le digital, levier de l'accélération de l'enseignement supérieur 54

La 5G, un enjeu B2B en Afrique 58

Le Covid-19, la confiance numérique et l'Afrique 60

CORONAVIRUS
Des mesures d'hygiène pour réduire les risques de cyberattaques 62

Vers la souveraineté numérique de l'Afrique 63

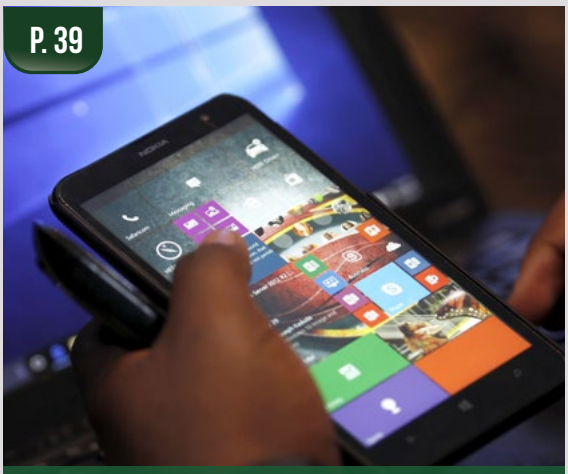
P.18

Abdoullah CISSE, Expert en droit du numérique : « La cybersécurité conditionne l'efficacité de la gouvernance numérique »

P. 30

FORMATION
Pourquoi envisager une carrière dans la cybersécurité ?

P. 39



CÔTE D'IVOIRE
La fraude au portefeuille électronique, une cyber-escroquerie redoutable

cio mag.com
LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

CIO Mag est édité par SAFREM Sarl

Directeur de publication :

Mohamadou DIALLO Mohamadou.diallo@cio-mag.com

Ont contribué à ce numéro

Mohamadou DIALLO :

Directeur de publication - Rédacteur en Chef.

Rédaction :

Véronique Narame, Camille Dubruelh (France);

Anselme Akeko (Côte d'Ivoire); Aurore Bonny (Cameroun);

Ousmane Gueye, Carlos Tobias (Togo);

Michaël Tchokpodo (Bénin)

Représentations deCIO Mag :

Maroc, Casablanca : Khadija - cio@cio-mag.com

Côte d'Ivoire : Anselme AKEKO : anselme.akeko@cio-mag.com
Tél: +225 08 56 47 26

Cameroun : Aurore BONNY : khadijahbenbonny@gmail.com

Sénégal : Abdoulaye DIALLO : abdoulaye33@hotmail.com

Tél : +221 77 595 50 02

Togo : Carlos TOBIAS : tobias.carlos@cio-mag.com

Tel : +228 90 26 38 54

Bénin : Michaël TCHOKPODO : michael@cio-mag.com

Régie Publicitaire et Abonnements :

info@cio-mag.com

www.cio-mag.com/sabonner

Experts :

Ibrahima Nour Eddine DIAGNE, Président d'African Performance Institute

Jean-Michel Huet, Associé, Afrique et développement International, Saleh Cherquaoui, Senior Manager, Bureau de Casablanca, Soukaina Kadiri & Marie Heipp, consultantes, bureau de Casablanca. Bearing Point

Arnaud Fléchard, CTO de Kleverware

Youssef Travaly, Vice-président du Next Einstein Forum

Direction artistique :CIO Mag
Impression : Rotimpres, Aiguviva Espagne
N° Commission paritaire 1110 T89651 N Dépôt légal Juin 2013

L'AFRIQUE EN CHIFFRES

2,5 %

Le continent perd environ 2,5% de son produit intérieur brut (PIB) après chaque mois de confinement, soit 65 milliards de dollars, selon les chiffres donnés par Mme Vera Songwe, la secrétaire exécutive de la Commission Economique pour l'Afrique (CEA).

177,7 millions de dollars

Le Togo a émis sur le marché de l'UEMOA, des bons de trésor de 177,7 millions de dollars ; soit 108 milliards de FCFA pour financer les besoins urgents liés à la pandémie de Covid-19.

89%

En Afrique subsaharienne, 89% des apprenants n'ont pas accès aux ordinateurs familiaux et 82% n'ont pas l'Internet.
Ces chiffres proviennent de l'Équipe spéciale internationale sur les enseignants, une alliance coordonnée par l'UNESCO.

15

Le Mali a récompensé les 15 premières Start-up ayant proposé des solutions digitales pour la lutte contre la pandémie de la Covid-19.
Ces dernières ont surtout collaboré à mettre en place la plateforme des solutions digitales du Mali.

73%

Selon Sofrecom, la filiale du Groupe Orange, entreprise de conseil et d'ingénierie spécialisée dans le secteur des télécommunications, plus de la moitié de ses collaborateurs estiment que les modes de travail et de fonctionnement ont été définis et adaptés au confinement. Soit au total, 73% des salariés qui souhaitent poursuivre le télé-travail.

10 millions

Le Camerounais Beaugas Orain Djoyoum, responsable de l'association Smart Click Africa, lance le projet « 10 millions Smart Citizens ». Objectif, former pendant 10 ans, 10 millions d'Africains pour la digitalisation du continent.

13,5%

Le groupe télécoms kényan, Safaricom, a annoncé en début d'année un taux de croissance de 13,5% de son chiffre d'affaires.
Pour 2019, le groupe a engrangé 262,5 milliards de shillings kényans. L'application M-Pesa contribue à elle seule à 12,6% de la croissance du groupe ; soit 33,6% du chiffre d'affaires en 2019.

6%

Pour lutter contre les crimes économiques et financiers, Atos recommande un usage efficient du numérique.
Sa plateforme modulaire MOSIP (Modular Open Source Identity Platform) permet d'avoir un impact jusqu'à hauteur de 6% sur le PIB.

Ils et elles ont dit ...

Hadja OUATTARA SANON, *Ministre du Développement de l'Economie numérique et des Postes du Burkina-Faso lors d'un E-Conf Challenge deCIO Mag.*
« Le digital est la bonne option. Après la crise, nous n'allons pas relâcher nos efforts. Le Burkina Faso mettra une partie des ressources disponibles dans la promotion de l'éducation à distance. »

Ndèye TICKÉ NDIAYE DIOP, *Ministre de l'Economie numérique et des Télécoms du Sénégal lors d'un E-Conf Challenge deCIO Mag.*
« Dans ce contexte de ralentissement général de l'activité économique, le digital est un moyen essentiel pour lutter contre la pandémie mais également pour assurer une continuité des activités économiques. »

Lacina KONÉ, *CEO de l'Alliance Smart Africa lors d'un E-Conf Challenge deCIO Mag.*
« La crise du Covid-19 a permis d'accélérer beaucoup d'initiatives digitales qui étaient dans les tiroirs et qu'on ne percevait pas comme étant un service essentiel. Les pays qui ont utilisé la technologie et les données à bon escient montrent une facilité à limiter la propagation de la maladie. »

Kamissa CAMARA, *Ministre de l'Economie numérique et de la Prospective du Mali lors d'un E-Conf Challenge deCIO Mag.*
« Nous sommes obligés d'utiliser les outils numériques dans cette situation de crise. Nous avons ainsi l'occasion de prouver que le secteur peut pallier certains défis de la crise sanitaire. »

Mohamed SAAD, *Président de l'Association des Utilisateurs des Systèmes d'Informations au Maroc (AUSIM) dans la revue «Cybersecurity Trends».*
« Cette crise sanitaire jamais vécue auparavant, et qui s'est propagée à la vitesse de la lumière, confinant des nations toutes entières, est en train de gagner du terrain et d'engloutir des milliards de dollars de pertes... mais surtout, elle est en train de détruire un capital confort, plaisir et bien-être ».

Les E-Conf Challenge pour mettre en lumière les innovations anti-Covid-19 en Afrique

L'apparition et la propagation du Covid-19 dans le monde bouleversent les relations humaines et freinent toutes les activités. L'administration publique, le secteur privé, le commerce, les transports,... tout tourne au ralenti. Les échanges commerciaux en mode B2C ont cédé la place au B2B via le digital. C'est pour l'heure la meilleure alternative pour préserver les relations humaines et maintenir la continuité des activités pendant cette crise. Presque tous les secteurs d'activité sont concernés. C'est dans ce contexte que CIO Mag, le média de référence sur les questions numériques en Afrique, a décidé de lancer ses E-Conf Challenge, pour donner la parole aux autorités ministérielles, aux décideurs et Start-up africaines du numérique.

L'objectif de ces rencontres virtuelles est double. Il s'agit d'une part de montrer comment le digital accélère le développement de l'économie et d'autre part de promouvoir le partage d'expériences pour faire émerger les meilleures pratiques. Cette initiative vient renforcer le lancement d'une carte interactive des différentes initiatives, pays par pays, disponible sur le site de www.cio-mag.com. Lors des trois premières éditions,CIO Mag a eu l'honneur de recevoir « à l'écran » cinq ministres africains : Mme. Hadja Ouattara Sanon, ministre du Développement, de l'Economie numérique et des Postes du Burkina-Faso, Mme. Ndèye Tické Ndiaye Diop, ministre sénégalaise de l'Economie numérique et des Télécoms. Ont également été invités : M. Léon Juste Ibombo, ministre de l'Economie numérique du Congo, Mme. Kamissa Camara, ministre de l'Economie numérique et de la Prospective du Mali et M. Yacine Oualid, ministre délégué chargé des Start-up de l'Algérie. Des entretiens dynamiques ponctués par des retours d'expériences thématiques avec des experts, Start-upeurs, Présidents d'universités... Les rencontres se poursuivent chaque semaine, avec de nombreux invités prévus. Tous ces entretiens sont à suivre en direct via Zoom. Inscrivez-vous à notre NewsLetter pour ne rien manquer !

Les webinaires sont ensuite mis en ligne et entièrement accessibles sur notre chaîne YouTube :CIO Mag TV.

SÉNÉGAL
« Le digital permet d'assurer la continuité des activités économiques »

Ndèye Tické Ndiaye Diop, ministre sénégalaise de l'Economie numérique et des Télécommunications, était l'invitée des E-Conf Challenge deCIO Mag. La responsable est revenue sur l'engagement de son pays dans la lutte contre le Covid-19 et a témoigné de l'importance du digital dans cette «guerre» contre le Coronavirus, ainsi que son impact dans l'après-crise.

Ndèye Tické Ndiaye Diop
Ministre de l'Economie numérique et des Télécoms

CIO Mag : Au regard de la situation actuelle, comment le digital peut être un facteur de développement dans le cadre du plan de continuité d'activité?

Ndèye Tické Ndiaye Diop : Dès l'apparition du Covid-19 au Sénégal, le 2 mars, le président Macky Sall a immédiatement pris la mesure de la contagiosité et de la létalité du virus et a adopté des règles sanitaires fortes pour protéger les citoyens et pour limiter la propagation de la maladie. Comme partout ailleurs, notre économie subit de plein fouet l'impact du Covid-19. Des secteurs comme le tourisme, l'hôtellerie, la restauration, les transports, le commerce, la culture, les bâtiments et travaux publics, entre autres, sont durement affectés.

Selon les nouvelles projections de l'OCDE, le durcissement des mesures pour ralentir la propagation du Coronavirus entraînera, à court terme, une baisse significative du PIB de nombreuses grandes économies. Les dernières estimations montrent que chaque mois de confinement provoque une perte de 2% de la croissance du PIB annuel.

Au Sénégal, la croissance économique, qui était soutenue depuis plusieurs années, a brutalement été freinée et passera très probablement de 6,8% à moins de 3%.

Dans ce contexte de ralentissement général de l'économie, le digital est un moyen essentiel pour lutter contre la pandémie, mais également pour assurer une continuité des activités économiques. Il s'agit de faire preuve de génie et d'utiliser les avantages des TIC pour atténuer les effets de cette crise sur l'économie sénégalaise.

La baisse des effectifs sur les lieux de travail s'est accompagnée d'une hausse massive du télé-travail partiel. Les outils numériques permettent aux agents de travailler efficacement à domicile et aident à limiter la propagation du virus. Grâce aux efforts consentis par les opérateurs de télécommunications, les entreprises et les Start-up ont bénéficié de la forte baisse des tarifs de connexion à Internet et au Mobile money.

L'enseignement à distance a également connu une forte progression, notamment dans les établissements privés.

Comment analyser les actions menées sur le continent avec les outils numériques pour maîtriser l'expansion de la pandémie ?

Le continent africain est en passe de démontrer son génie et sa résilience dans la gestion de cette crise.

Ndèye Tické Ndiaye Diop,
Ministre de l'Economie numérique et desTélécoms

INTERVIEW

Et le numérique reste un atout incontournable pour la maîtrise de la pandémie du Covid-19 et l'amélioration des conditions de vie et de travail.

L'Afrique a innové en produisant des cartes pour suivre l'évolution de la pandémie et des applications de tracking des cas de Covid-19. Elle a aussi tiré partie de l'IOT pour installer des cabines de lavages de mains connectées et pour produire et distribuer des masques. Le continent a démontré sa solidarité car la majorité des initiatives a été développée, à titre bénévole, par les communautés. Pour paraphraser Pierre Mauroy, *« la crise n'est pas comme une maladie dont on ne peut sortir : elle est comme une sorte de nouvelle naissance »*. Je reste ainsi convaincue que cette crise est une opportunité de renaissance pour l'Afrique.

Quelle a été la stratégie de votre ministère pour mettre en place un plan de riposte avec les outils numériques et pour coordonner les actions avec l'écosystème, les autres ministères et les agences de l'Etat ?

Pour marquer mon soutien et ma solidarité au Chef de l'Etat et au Gouvernement dans la lutte contre cet ennemi invisible, j'ai réuni les acteurs du secteur du numérique afin d'optimiser la coordination des actions. Un comité de suivi a été mis en place pour évaluer régulièrement les besoins en fonction de l'évolution de la situation. Une coalition dénommée #DaanCovid19 ou *« Riposte digitale contre le Covid-19 au Sénégal » a été mise en place.*

Elle regroupe tous les acteurs de l'écosystème : secteurs public et privé, société civile, universitaires.

L'objectif est d'utiliser les possibilités offertes par les TIC pour appuyer les actions prioritaires de l'État, telles que définies par le ministère de la Santé et de l'action sociale. Il s'agit de fédérer, de façon bénévole, les meilleures ressources digitales du pays, afin d'endiguer la pandémie de Covid-19 au Sénégal grâce au numérique.

Le ministère de l'Economie numérique apporte sa contribution au ministère de la Santé et de l'action sociale, et répond aux besoins exprimés en sécurisant les réseaux et les services de communications électroniques. Le but est de garantir la disponibilité du réseau téléphonique, de l'Internet et du Mobile Money, et d'assurer une bonne qualité de services sur l'ensemble du territoire.

Parmi les solutions digitales mises à disposition pour la gestion médicale et sociale de la pandémie, je peux citer le système d'information médical, d'enregistrement et de traitement des données, le centre d'appels, la géolocalisation des cas, etc.

Globalement, le secteur du numérique a contribué à hauteur de plus de quatre milliards FCFA.

Pour toutes ces actions, quels sont les obstacles et les résistances que vous avez rencontrés ? Comment avez-vous réussi à les contourner ou à les résoudre ?

Comme dans tout changement, les résistances ont été le fait d'acteurs qui ont dû s'adapter à des outils ou des méthodes de travail jusque-là méconnus. Et ce n'est pas toujours facile car cela demande beaucoup d'agilité.

Fort heureusement, les acteurs ont su s'adapter à la forte demande de services de communications, laquelle est liée au télé-travail et à la limitation des déplacements des personnes.

D'ailleurs, il a fallu augmenter la bande passante disponible pour l'accès à Internet, améliorer la surveillance des réseaux, renforcer la qualité de services et s'adapter aux outils de travail collaboratif.

En sus des actions gouvernementales, comment êtes-vous parvenue à travailler avec les Start-up et à les impliquer dans cette lutte contre la pandémie ?

Le Sénégal dispose d'une loi sur les Start-up et mon département a initié une cartographie de ces structures appelées à être accompagnées par cette loi. Une association

dénommée « Sen Start-up » a été mise en place. Elle regroupe une cinquantaine de Start-up et est en contact permanent avec mes services. Ainsi, dès l'entame de la maladie, j'ai convoqué le secteur privé TIC national, les incubateurs et les représentants de l'association Sen Start-up, afin de mieux organiser la riposte digitale.

La mobilisation des Start-up, qui sont efficaces dans les solutions digitales innovantes, a été facilitée par les réseaux sociaux et les mailing-listes existants, ainsi que par les corporations de métiers.

Des plateformes d'inscription sont initiées dans les réseaux et des lettres officielles invitent à participer à l'initiative. Elles sont envoyées aux responsables des structures. Plusieurs Start-up ont répondu positivement et ont accepté de mettre gracieusement leurs applications au service de la lutte contre la pandémie.

Quels enseignements tirez-vous de cette crise sanitaire ?

D'une façon générale, cette crise sanitaire sans précédent confirme les adages « *Ensemble, nous pouvons soulever des montagnes* » et « *Mieux vaut prévenir que guérir* ». Ensuite, nous confirmons que le numérique est un atout majeur pour le développement de la santé digitale. Il accélère les procédures et améliore le rendement du corps médical.

C'est un moyen efficace pour sensibiliser les populations et plus généralement pour communiquer. Son apport est déterminant dans tous les secteurs prioritaires : éducation, bancaire, commerce, etc. Enfin, le numérique occupe une place prépondérante, notamment dans les transactions électroniques et le e-commerce.

De votre point de vue, le numérique en sortira-t-il renforcé ?

Cette crise sanitaire mondiale va indéniablement accélérer la transformation numérique déjà engagée dans nos pays. Il convient d'ailleurs de souligner que le Président a très tôt compris l'importance du numérique en l'intégrant au Plan Sénégal Emergent (PSE), comme levier majeur de la transformation structurelle de l'économie nationale. Cette crise a fortement boosté l'utilisation du digital, avec notamment le télé-travail, l'utilisation accrue de la visioconférence, des systèmes de messagerie, de télémédecine, d'e-commerce et de services de paiement mobiles.

Ainsi, pour anticiper d'éventuelles crises, nous allons travailler avec l'ensemble des acteurs pour renforcer :

- Le développement des réseaux intranet de l'administration ;
- L'offre digitale des services publics (E-Gov à développer davantage) ;
- Le développement des télé-services (téléenseignement, télé-médecine, conférences en ligne...) ;
- Le développement des services e-money et e-commerce ;
- La connectivité en augmentant les bandes passantes des réseaux et des ressources Internet ;
- La mise à niveau des cadres législatifs et réglementaires pour s'adapter au changement rapide de paradigme ;
- La sécurité des données.

Je rappelle que le Sénégal a enregistré de nombreuses avancées en matière de développement de l'économie numérique, parmi lesquelles :

- Un cadre juridique favorable ;
- Un taux de pénétration de l'Internet de 74.31% à fin décembre 2019 ;
- Un taux de pénétration du mobile de 110.63% à même date ;
- Un réseau de l'intranet administratif ayant éprouvé la capacité de son système de visioconférence (conseil des Ministres) ;
- Un système de messagerie en cours de généralisation au niveau de l'administration ;
- Une bonne connectivité avec la présence de câbles sous-marins tels qu'Atlantis II, SAT3, ACE, MainOne ;
- L'existence d'un point d'échanges Internet pour minimiser les coûts et garder le trafic domestique en local.

Je demeure convaincue que tous ces avantages comparatifs constituent un socle susceptible de contribuer à la pérennisation des nombreuses initiatives actuellement menées au Sénégal dans le cadre de la lutte contre le Covid-19.

Pour conclure, je pense que l'Afrique devrait saisir cette opportunité pour renforcer les initiatives régionales dans le domaine du numérique, à travers les Communautés régionales, l'Union africaine et Smart Africa. Car les TIC, de par leur caractère transversal, sont un véritable outil d'intégration économique et sociale pour le continent.

Propos recueillis par Mohamadou Diallo

ALGERIE
« Transformer le pays en Start-up Nation, c'est notre ambition »

Yacine Oualid, ministre algérien délégué aux Start-up, est intervenu dans les E-Conf Challenge deCIO Mag. Le ministre a évoqué les mesures prises en Algérie pour lutter contre le Covid-19 et a analysé la réactivité des Start-up algériennes pour répondre à cette crise.

Yacine Oualid
Ministre délégué chargé des Start-up

CIO Mag : En Algérie, quel rôle joue le digital dans la lutte contre le Coronavirus ?

Yacine Oualid : J'aimerais tout d'abord souligner l'importance de la data dans cette crise sanitaire. L'Algérie est le plus grand pays d'Afrique (en terme de superficie, NDLR). L'enjeu spatial est important à maîtriser.

Pour mieux analyser la pandémie de Covid-19, il fallait donc faire remonter suffisamment de données, afin de comprendre son évolution dans toutes les régions du pays. Et cela a été rendu possible par la coordination de différents départements ministériels, notamment la Santé et l'Intérieur, et via la mise en place d'une cellule de crise.

Concernant les outils de tracking, comment se positionne l'Algérie ? Et comment mettre cela en place tout en garantissant la protection des libertés des citoyens ?

Nous avons reçu beaucoup d'initiatives dans ce sens et avons mis en place des outils de tracking. Ainsi, le ministère de la Santé a pu faire remonter des données vers la cellule de crise, afin de suivre les personnes atteintes par le Covid-19 et les prendre en charge.

C'est dans l'intérêt de la santé publique. Dans ce contexte, les citoyens ont fait confiance et ont donc donné leurs informations personnelles pour répondre à la gestion nationale de la pandémie.

Quel rôle ont joué les Start-up du pays pour aider à contrer la propagation du virus ? Comment le gouvernement a-t-il travaillé avec ces acteurs ?

L'accélération du processus de transformation numérique a été l'une des plus importantes missions du nouveau gouvernement, et ce, avant même le début de l'épidémie. Ce processus ne peut se faire sans l'implication des innovateurs, notamment les jeunes entrepreneurs et les Start-up. Nous avions déjà engagé plusieurs actions pour travailler avec l'écosystème.

Depuis le début de la pandémie, nous avons assisté à une avalanche d'initiatives. Cela a été une véritable opportunité pour les Start-up de démontrer ce qu'elles valent et ce qu'elles savent faire.

Aujourd'hui, nous devons plus que jamais profiter de cette nouvelle énergie dont regorge l'Afrique. Elle prouve qu'on peut faire des miracles en très peu de temps. Le numérique a pris tout son sens dans cette crise. Ce n'est plus une option mais une nécessité.

Le virage du digital est civilisationnel. C'est donc une grande responsabilité qui repose sur nos épaules.

INTERVIEW

Yacine Oualid
Ministre délégué
chargé des Start-up

Dans ce contexte de crise sanitaire et économique, quelles innovations et quelles solutions proposées par les Start-up vous ont le plus interpellé ?

Les Start-up ont occupé une place très importante dans la lutte contre le Coronavirus. De façon spontanée, de nombreuses Start-up sont venues proposer leurs solutions aux ministères de la Santé, du Commerce, etc. Nous avons été extrêmement proches de la communauté digitale dans cette crise et nous avons mis en place différentes initiatives pour travailler avec elle autour de la réponse au Coronavirus. Les incubateurs, notamment, sont très actifs. Nous les avons par exemple accompagnés dans l'organisation de hackathons. Cela a permis de dégager des solutions absolument incroyables dans le domaine des respirateurs artificiels, des solutions de Big data, de géotrackings, etc.

Au niveau des Start-up, l'une d'entre elles a par exemple lancé une plateforme de télé-consultation et télé-médecine, à partir de laquelle ont eu lieu des milliers de consultations. Nous avons par ailleurs eu un gros problème de transport du personnel soignant. Et pour régler cela, les VTC algériens (TemTem, Wesselni ou encore PickmeApp, NDLR) se sont mobilisés pour transporter gratuitement les soignants. Ce ne sont là que quelques exemples. Il y a tellement de solutions proposées qu'il est difficile de n'en sélectionner qu'une ou deux !

Cette collaboration entre les autorités et les Start-up en Algérie a-t-elle vocation à perdurer au delà de la crise ?

Le sujet de la Start-up occupe une place toute particulière au sein du Gouvernement, à telle enseigne qu'un nouveau département ministériel dédié aux Start-up a été créé et que je représente. Notre vision, c'est de faire de l'Algérie une Start-up Nation. Pour promouvoir les Start-up algériennes, nous sommes en train de travailler sur un cadre réglementaire. Nous travaillons également sur les mécanismes de financement afin qu'ils soient plus adaptés aux Start-up.

La pandémie de Covid-19 nous a certes beaucoup retardés dans notre travail mais, en parallèle, elle nous motive encore plus pour matérialiser nos objectifs. Concrètement, nous continuons d'avancer et nous croyons que les objectifs fixés - à savoir la mise en place du cadre réglementaire, la fixation des facilités fiscales et parafiscales, l'accès aux marchés publics et les financements - seront atteints cette année. Au-delà de ces mesures, nous promettons aux Start-up, qui se sont mobilisées de façon incroyable dans cette crise, de garantir un appui des autorités dans la commande publique. Ceci afin qu'elles soient la pierre angulaire de la nouvelle économie algérienne que nous voulons construire.

« Le numérique n'est plus une option mais une nécessité. Le virage du digital est civilisationnel »

Comptez-vous sur une dynamique africaine pour faire de l'Algérie une Start-up nation ?

Notre nouveau ministère a une grande responsabilité et nous accordons également beaucoup d'importance aux synergies avec les pays voisins et avec l'Afrique toute entière. Il faut que nous puissions consommer africain lorsqu'il s'agit de numérique et d'innovations. La diaspora a aussi tout son rôle à jouer.

Nous voulons que les Algériens, formés en Europe ou aux Etats-Unis, puissent nous faire profiter de leur expérience dans leurs domaines respectifs, mais aussi leur permettre d'investir et d'entreprendre en Algérie. Pour cela, nous sommes en contact permanent avec la diaspora. Nous avons même un département ministériel qui lui est dédié. La diaspora est une véritable richesse pour nous, car elle est tout particulièrement dévouée à l'intérêt de l'Algérie.

Propos recueillis par Mohamadou Diallo et Camille Dubruelh

CYBERSÉCURITÉ

Les actes de cybercriminalité ont-ils atteint leur pic en Afrique ?

La pandémie due au Coronavirus accélère la propagation des actes criminels informatiques. Déjà, avant le déclenchement de cette crise, la cyberdéfense du continent africain comportait des failles. Pour l'heure, il existe très peu de rapports à l'échelle du continent, alors qu'ailleurs, des états des lieux sont produits. En réalité, ce secteur est secoué par d'autres maux que ceux liés au Covid-19. En cause, le manque de données fiables et d'infrastructures robustes. Dans ces conditions, l'Afrique a-t-elle les moyens de mener la bataille de la cybersécurité exacerbée par la guerre contre le Coronavirus ?

Souleyman Tobias

Dans une publication récente, Orange Cyberdéfense faisait état d'une augmentation de 20 à 25% des cyberattaques en France avec la crise sanitaire du Coronavirus. Les secteurs les plus vulnérables sont ceux de la santé, de la grande consommation, des banques, etc. Ces informations sont importantes pour établir un scénario de riposte et prévenir les risques. Les infrastructures de veille, de solution et de prévention étant soit inexistantes, soit jeunes, le continent africain n'a pas les coudées franches pour faire face à la multiplication des cybers risques, en cette période de crise sanitaire.

L'augmentation à l'échelle mondiale de la cybercriminalité est proportionnelle à la peur due au Covid-19. Les criminels informatiques profitent donc de la panique générale et de l'impréparation des entreprises et des individus pour exploiter au maximum les failles informatiques.

Elles sont très souvent accentuées par les maladresses liées justement à la panique du moment.

En l'état de la situation, il est difficile d'établir l'impact réel de cette crise sur la cybersécurité en Afrique. Mais, les données qui existaient avant cette crise n'étaient déjà pas des plus rassurantes.

Dans un rapport publié en 2018, l'Africa Cyber Threat Intelligence Report (ACTIR) révélait qu'au moins 96% des incidents de sécurité liés à Internet n'avaient pas été signalés et que plus de 70% des organisations ne s'étaient pas informées des tendances de la cybersécurité sur le continent. Les auteurs du rapport allaient jusqu'à dire que des agences officielles ignoraient l'étendue du risque numérique.

Et pourtant, depuis déjà plus d'une décennie, le continent s'est lancé dans plusieurs projets de digitalisation, lesquels impliquent le plus souvent des services sensibles. L'étude de l'ACTIR commandée dans le cadre de la Conférence africaine sur la cybersécurité (ACSC) a aussi révélé que *« la cyber-vulnérabilité du continent est accrue par la faiblesse des architectures de sécurité, par la rareté du personnel qualifié, le manque de sensibilisation et de coordinations des réglementations dans les pays africains »*. Toutes les sources dignes de foi s'accordent à dire que sur le terrain de la cyberdéfense, l'Afrique était d'ores et déjà vulnérable, du moins un peu plus que les autres continents.

La menace a-t-elle évolué ?

C'est un secret de polichinelle ! Car, comme nous l'avions déjà signalé, les données tangibles sont difficiles à rassembler. Peut-on cependant en déduire, à l'aune de la situation d'avant crise, que le continent n'était pas forcément le mieux préparé ? En 2017, l'Afrique perdait 3,7 milliards de dollars à cause des crimes informatiques. Combien le continent risquerait-il de perdre avec la pandémie du Coronavirus ? Aucune donnée actualisée ne l'évoque.

Avant le Covid-19, l'Afrique était à l'œuvre pour viabiliser sa stratégie numérique. Un grand nombre de pays venait tout juste de mettre en place un Centres d'alerte et de réaction aux attaques informatiques (CERT) national, avec des lois sur la cybersécurité.

Dans un rapport publié en octobre 2018, à l'issue d'un atelier régional de l'Union économique et monétaire ouest-africaine (UEMOA) sur le commerce électronique en partenariat avec l'Union africaine, la commission de l'UA prenait la mesure de la fragilité de la cyberdéfense sur le continent.

« L'Afrique est le continent le plus émergent en termes de développement des infrastructures et de concurrence sur le marché… Mais, sans des politiques et des cadres règlementaires favorables, aucune garantie n'est envisageable pour optimiser les services, les accès et les coûts », pouvait-on lire dans ce rapport de quinze pages.

Des experts en cybersécurité ont également mis en évidence que *« 80% des PC du continent africain sont infectés par des virus et d'autres logiciels malveillants »*. Ils ont aussi fait référence à un rapport de Symantec, lequel révélait en 2012 que le nombre de cyberattaques ciblées en Afrique avait augmenté de 42%.

Comment rectifier le tir ?

Les raisons qui expliquent l'écart entre les cybers menaces et la réponse africaine sont connues. Le rapport 2018 de la commission de l'UA, cité plus haut, identifiait certaines de ces raisons.

Au nombre d'entre elles, les lacunes qui plombent les projets de digitalisation sur le continent, le faible niveau de la sensibilisation sur le sujet, le manque de financement et de collaboration entre gouvernements et spécialistes, le manque de compétences… Or, avec la démocratisation des usages, les risques ne cessent d'augmenter.

Entre Etats, la collaboration est également loin d'être celle que l'on pourrait escompter.

En Afrique, il n'existe pas de grands projets régionaux de cyberdéfense connus. Dans son rapport, la commission de l'UA avait enquêté sur les tendances de la cybersécurité et de la cybercriminalité à l'échelle continentale. Seuls 60% des pays avaient répondu à l'enquête (soit 60% de sondés).

La commission de l'UA exprimait *« une volonté politique claire d'entraide mutuelle internationale dans la lutte contre la cybercriminalité »*. Dans une interview accordée à CIO Mag en 2018, Chrysostome Nkoumbi-Samba, fondateur d'Afrik@ Cybersécurité déclarait :

« La cybersécurité doit désormais être considérée comme l'une de nos assurances collectives pour l'avenir. Sans celle-ci, il manque un maillon à la chaîne globale de business des entreprises. Nous sommes à un moment charnière, où il faut dépasser le partage de la peine. Tous les managers, toutes les directions exécutives des entreprises doivent prendre conscience du risque cyber actuel. Ce n'est pas un problème de subir les attaques. Mais ce qui est problématique, c'est soit de ne pas le savoir, soit de ne pas être capable de trouver des moyens de les parer. Cet enjeu concerne toute la chaîne de décision de l'entreprise. Tout ce qui va dans le sens de cette meilleure prise en compte des enjeux de la cybersécurité me paraît être une excellente initiative. Et, sur ce point, il faut jouer collectif… ».

Une déclaration qui sonnait comme un appel à l'action. Le continent africain, qui s'est engagé dans une transformation digitale, sait qu'il n'a plus d'autre choix. Face aux menaces qui fragilisent ses infrastructures, les conséquences économiques s'évaluent chaque année à des milliards de dollars.

Des politiques de cyberdéfense émergent sur le continent pour contrer ces attaques. De plus en plus d'Etats adoptent des lois claires contre la cybercriminalité et en faveur de la protection des données sensibles et personnelles.

Des datacenters publics sont en construction ici et là pour assurer un début de souveraineté numérique aux pays. Des CERT se mettent en place, tant au niveau pays qu'entreprises. La cybersécurité semble désormais faire partie intégrante des mécanismes de déploiement des projets digitaux.

De même, l'Afrique a pris conscience du manque de ressources locales dans le secteur de la cybersécurité.

Pour y répondre, des écoles s'ouvrent, comme c'est le cas de l'école régionale de Dakar, au Sénégal, ouverte en 2018, sans oublier celles du Maghreb, en Tunisie ou au Maroc. Aussi, les forces de sécurité du continent s'entourent de services de cybersécurité. Ce sont des signaux encourageants !

Une étude de Cybersecurity Ventury, citée dans un article de *Jeune Afrique* de décembre 2018, prévoyait 3,5 millions d'emplois à pourvoir dans la cybersécurité, d'ici à 2021, à l'échelle mondiale. Le continent africain s'est-il armé pour faire face à ce besoin ?

La situation provoquée par la pandémie de Coronavirus remet à l'ordre du jour cette question.

Orange, partenaire de confiance des entreprises et des institutions pour travailler à distance en toute sécurité

@orangeafrica

Vous rapprocher
de l'essentiel

orange™

« La cybersécurité conditionne l'efficacité de la gouvernance numérique »

Abdoullah Cisse est spécialiste en droit du numérique et en droit des affaires et membre du Groupement d'expertises Carapaces. Il a contribué à l'introduction du numérique dans plusieurs organisations et États d'Afrique francophone. Ce juriste est membre titulaire de l'Académie nationale des Sciences et Techniques du Sénégal et membre associé de l'Académie internationale de droit comparé. PourCIO Mag, il revient sur les enjeux relatifs à la cybersécurité au niveau des Etats du continent et sur les défis à relever. Interview.

Abdoullah Cisse
Expert en droit du numérique

CIO Mag : En termes de cybersécurité, quels sont les défis pour les Etats africains ? L'Afrique est-elle le nouveau foyer des cyberattaques ?

Abdoullah CISSE : Dans un contexte de dématérialisation globalisée, les cybermenaces constituent un phénomène multidimensionnel et multiforme. Il met en péril le patrimoine numérique et culturel des individus, des organisations et des Nations, au point de compromettre la pérennité et la souveraineté des Etats et des gouvernements.

Le défi actuel des États africains est multiforme : il est politique, économique, socioculturel, technologique, environnemental et juridique. En d'autres termes, la cybersécurité conditionne aujourd'hui la transparence et l'efficacité de la gouvernance numérique, ainsi que la protection de l'environnement.

Le développement de l'économie numérique et du commerce électronique est largement tributaire des garanties de sécurité, qui nourrissent la confiance des usagers.

Cette cybersécurité présente une dimension culturelle très importante dans des environnements peu numérisés, où la culture numérique demande à être promue.

La faiblesse des investissements pour renforcer le plateau technologique rend subsidiaire la prise en charge de la cybersécurité. L'ensemble de ces paramètres tarde à être pris en charge dans le droit positif de la plupart des États africains.

Cela appelle d'abord à une prise de conscience de la réalité du besoin de cybersécurité. Et des moyens à mobiliser sur les plans humain, logistique et financier au regard de l'impact énorme des questions de cybersécurité sur la souveraineté et la pérennité des États africains.

En l'absence de stratégies à long terme et de véritables politiques de cybersécurité dans la plupart des pays, et à défaut de législations appropriées, il est normal que ces États soient « des paradis pénaux ». Et, partant, des proies faciles pour les cybercriminels. Tous les États sont vulnérables, mais le niveau de vulnérabilité est plus élevé en Afrique pour les raisons que nous venons d'évoquer.

INTERVIEW

Abdoullah Cisse
Expert en droit du numérique

Pensez-vous que les enjeux sont totalement pris en considération au niveau des Etats et des entreprises africaines ?

Des progrès notables sont enregistrés, au plan régional, dans le cadre de l'harmonisation des cyberlégislations. On peut souligner les normes communautaires sur les transactions électroniques, la protection des données personnelles et la lutte contre la cybercriminalité, adoptées dans les espaces UEMOA-CEDEAO et CEEAC-CEMAC. Au niveau de l'Union africaine, l'adoption, en juin 2014, de la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel constitue une avancée majeure. Mais, elle est encore limitée par le fait qu'elle n'a pas encore obtenu les quinze ratifications nécessaires à son entrée en vigueur.

Pourtant, une véritable stratégie d'influence de certaines organisations régionales - comme la CEDEAO ou l'OHADA - aurait suffi, par une mobilisation soutenue de ses membres, à accélérer la ratification. Et aurait, en conséquence, favorisé l'entrée en vigueur de la Convention de Malabo.

Dans l'espace OHADA, les dernières réformes de 2011 à 2014 ont permis d'introduire le numérique, notamment dans le droit des sûretés, le droit des sociétés et le droit commercial général, avec l'important projet sur l'informatisation du registre du commerce et du crédit mobilier.

Toutes ces initiatives témoignent aujourd'hui d'une certaine prise de conscience, de la part des organisations africaines, des enjeux de cybersécurité et de promotion de l'économie numérique.

Toutefois, au regard de la vitesse et de l'immensité des progrès technologiques, des efforts restent encore à fournir de la part des gouvernements, du secteur privé et des organisations de la société civile en matière de cybersécurité.

Il serait important d'organiser le plaidoyer à l'intention des gouvernants africains, car sans le passage assumé à la république numérique, la question de leur aptitude à gouverner, à légiférer, à protéger leurs citoyens et leurs biens, bref à être souverains, cette question se posera de plus en plus.

La Convention de Malabo va-t-elle assez loin, notamment sur la protection des données à caractère personnel ?

Il est important de rappeler que la durée moyenne pour l'entrée en vigueur d'une convention africaine est d'une décennie. L'organisation est donc dans son agenda normal sauf qu'un tel rythme ne s'accommode guère avec celui de progression du numérique.

A son adoption, certaines dispositions de la Convention de Malabo en matière de protection des données, de cybersécurité et de lutte contre la cybercriminalité étaient en phase avec les innovations numériques. Mais à l'heure actuelle, beaucoup de ces dispositions commencent à entrer dans l'obsolescence.

En réalité, si la convention a certes été signée en 2014, l'essentiel du texte était déjà disponible en 2010-2011, ce qui veut dire que son âge réel est de dix ans.

Dans sa forme actuelle, elle peut surtout servir dans les États qui tardent à légiférer en matière de cybersécurité. Certains n'ont pas hésité à s'en inspirer dans leurs réformes, alors même qu'ils ne l'ont pas ratifiée, ce qui montre l'utilité de l'instrument et la pertinence de son contenu.

Récemment, des accusations d'écoutes au siège de l'Union africaine ont été proférées. Si Huawei s'en est défendu, on a en revanche peu entendu la version de l'UA. Quelle est votre analyse de la situation ?

Tant qu'un cadre éthique et transparent ne régira pas la cybersécurité au plan national, continental et international, il sera difficile de se prononcer sur des questions de cette nature en raison de leur extrême complexité. Lorsqu'on dépend de l'aide pour construire sa propre maison, lorsqu'on n'a pas son mot à dire sur l'éthique des entreprises qui construisent les infrastructures technologiques dans notre propre maison, lorsqu'on ne dispose pas des capacités pour évaluer les interventions de ces entreprises et pour répondre en cas de dysfonctionnements, dans des circonstances pareilles, disais-je, le silence peut, en effet, être une posture accommodante. Cela étant, il serait utile d'approfondir les enquêtes sur cette question sensible.

Pensez-vous que l'Afrique est le continent le plus vulnérable ?

La cybercriminalité est un phénomène global et transfrontalier. A chaque société, ses profils de cyberdélinquants et de victimes. En Afrique, les cybercriminels ont longtemps considéré le continent comme un lieu « providentiel » pour commettre leurs actes criminels, en raison de la faiblesse des infrastructures de sécurité, de l'insuffisante culture numérique et de l'absence des cadres juridiques adéquats qui concourent à l'impunité.

On y retrouve presque toute la panoplie des infractions connues dans le cyberespace : cyberescroquerie - arnaques aux sentiments (arnacoeur), chantage à la vidéo (sextorsion), faux visas, fausses offres d'emploi et de bourses d'études - et piratage de boîte mail (phishing et hameçonnage). Et même le ransomware (logiciel de rançon), etc.

En l'absence de CERT (computer emergency response team), dans la plupart des États africains, il est difficile de tracer tous les cas de cybercriminalités et de mesurer le degré d'implication des non-Africains dans la cybercriminalité qui se déroule en Afrique.

Des pays font-ils figure d'exemples en termes de cadre légal autour de la cybersécurité ?

Selon Le Global Cybersecurity Index (GCI), le cadre légal ne suffit pas à lui seul à déterminer les capacités d'un Etat à répondre efficacement aux cybermenaces. Cette référence, mise en place par l'Union internationale des télécommunications, mesure l'engagement des pays à l'égard de la cybersécurité au niveau mondial. Et consiste à faire prendre conscience de l'importance et des différentes dimensions du problème. La cybersécurité est ainsi évaluée selon cinq piliers : mesures juridiques, mesures techniques, mesures organisationnelles, renforcement des capacités et coopération. Selon le rapport GCI de 2017, trois Etats sortent du lot en Afrique. Il s'agit de l'Ile Maurice, du Kenya et du Rwanda. D'autres États font, certes, des efforts et méritent d'être encouragés.

Que préconisez-vous en tant qu'expert ?

Avons-nous d'autre choix que d'accélérer volontairement et consciemment le passage au numérique, pour faire de la république numérique souveraine une réalité africaine ? Au-delà des aspects négatifs de la situation sanitaire qui prévaut présentement, la pandémie offre aux Africain.e.s une opportunité extraordinaire pour promouvoir le commerce électronique, les moyens de paiement numérique, télé-travail, télé-médecine, la formation ouverte et à distance, la dématérialisation des procédures et des formalités administratives et bien sûr l'accès universel au haut débit.

En matière de technologies numériques appliquées à tous les domaines de la vie économique, sociale et culturelle (notamment en matière d'interopérabilité, de big data, de systèmes d'information, de cybersécurité, etc.), l'expertise nationale nichée dans les Start-up et les organisations nationales peut être véritablement mise à profit. Mais, pour entretenir la confiance des citoyens, il ne faudra pas baisser la garde et continuer à ériger en impératif catégorique la sauvegarde de la vie privée des personnes, la sécurité numérique et la lutte, sous toutes ses formes, contre la cybercriminalité.

Propos recueillis par Camille Dubruelh

AFRIQUE

Des cadres légaux adaptés aux menaces cybersécuritaires ?

Protéger les Etats, les entreprises et les citoyens de la menace cybersécuritaire passe en premier lieu par l'adoption de cadres légaux. Au niveau panafricain, la cybersécurité est régie par la Convention de Malabo, adoptée en 2014. Mais de nombreux pays du continent ne l'ont jamais signée ou ratifiée. Si certains d'entre eux ont pris la mesure de la menace et adopté des textes de lois dans ce cadre, le continent affiche un retard certain en termes de législations.

Camille Dubruelh

« Face à l'actualité de la cybercriminalité, qui constitue une véritable menace pour la sécurité des réseaux informatiques et pour le développement de la société de l'information en Afrique, il est nécessaire de fixer les grandes orientations de la stratégie de répression de la cybercriminalité ». Convention de Malabo – 2014.

L'Afrique est entrée de plain-pied dans l'ère numérique. Le gap, qui séparait l'Afrique du reste monde, se comble d'année en année du fait d'une croissance forte et soutenue et grâce à la pénétration des marchés mobile et Internet. Les risques cybernétiques n'en constituent pas moins un fléau, qui pourrait saper ce secteur hautement stratégique. A l'heure actuelle, les pays africains sont loin d'avoir pris la mesure de la menace cybersécuritaire et accusent, pour la plupart, un retard certain en matière de lutte contre la cybercriminalité et dans la protection des données des citoyens.

Notamment dans la mise en place de la conformité et des cadres légaux nécessaires pour sécuriser

les échanges. Ces manquements engendrent un manque à gagner colossal... Plusieurs millions de dollars échappent ainsi chaque année aux Etats et aux entreprises.

L'Union Internationale des Télécommunications a publié l'Indice de la sécurité dans le monde pour 2017 (GCI-2017), qui permet de mesurer l'engagement des 193 Etats membres de l'UIT en faveur de la cybersécurité. Et les chiffres sont édifiants.

En 2017, les pertes annuelles imputables aux cyberattaques se chiffraient par exemple à 649 millions de dollars pour le Nigeria, à 210 millions pour le Kenya ou encore à 157 millions pour l'Afrique du Sud. D'un point de vue global, en 2017, l'étude estimait les pertes pour le continent à 3,7 milliards de dollars.

Ces chiffres ne tiennent pas compte de certaines attaques subies par les Etats et les grandes entreprises, qui préfèrent les passer sous silence pour éviter de s'exposer aux critiques et préserver leur image.

« Il y a quelques années, on se demandait si le continent était suffisamment doté en outils numériques. Aujourd'hui, l'Afrique est en plein dans le cyberespace, mais la question est de savoir si elle est assez protégée au plan de la cybersécurité. La menace est là et son évolution n'a pas de limite, car elle dépend de l'ingéniosité des cyber-attaquants », analyse Elhadji Oumar Ndiaye, Docteur en Droit, spécialiste des problématiques liées à la cybersécurité et à la cybercriminalité.

Alors que faire pour protéger les économies et les populations de cette menace constante ? Pour les Etats, la priorité, pour y faire face, est de se doter des instruments juridiques adéquats.

La Convention de Malabo, un texte peu appliqué

« Sur le continent, la prise de conscience est là. Les autorités étatiques savent qu'il est nécessaire de mettre en place des stratégies et des législations. Les entreprises prennent également conscience de cette cybermenace », estime le spécialiste. Selon lui, les acteurs du secteur ont commencé à travailler sur ces questions dès le début des années 2000. Le Burkina Faso (2004) ou encore le Sénégal (2008) ont été parmi les premiers Etats à se saisir de la question et à adopter des législations pour protéger les données de leurs citoyens.

A l'échelle de l'Union africaine, le texte de référence reste, aujourd'hui encore, la Convention de Malabo, adoptée en 2014. Sectionnée en plusieurs chapitres, elle propose un cadre légal très large pour permettre aux Etats de réguler les transactions électroniques, la protection des données personnelles et la lutte contre la cybercriminalité. Le problème, c'est qu'aujourd'hui, seuls 13 pays du continent l'ont signée (Bénin, Tchad, Comores, Congo, Ghana, Guinée-Bissau, Mauritanie, Sierra Leone, São Tomé-et-Príncipe, Zambie, Sénégal, Ile Maurice, Togo) et trois l'ont ratifiée, à savoir le Sénégal, l'Ile Maurice et plus récemment le Togo, en 2019.

«Cela ne signifie pas qu'il n'y a aucun cadre dans les autres Etats, rassure Elhadji Oumar Ndiaye. Beaucoup de pays n'ont pas ratifié le texte, mais s'en inspirent pourtant dans leurs législations nationales et transposent ces principes», poursuit-il, citant l'exemple du Congo. Ce pays a adopté un arsenal législatif autour de ces questions, sans avoir encore ratifié la convention. *«Il y a peut-être un problème de leadership, au sein de l'Union africaine, pour œuvrer à l'effectivité de cette Convention»*, poursuit le Docteur en droit.

Adapter les législations aux nouvelles menaces

L'autre problématique est de savoir si la Convention de Malabo est assez moderne pour répondre à l'expansion des nouvelles technologies et aux nouvelles menaces induites. *« C'est un texte qui s'inscrit dans une optique d'harmonisation à l'échelle du continent. Il a été rédigé de façon assez large pour englober le maximum de situations possibles et permettre ainsi aux Etats d'adapter les législations par rapport à l'évolution des technologies »*, explique Elhadji Oumar Ndiaye. Mais, le cyberespace connaît des révolutions successives et ce, de façon exponentielle.

Ainsi, *« il serait utile que cette Convention soit revue, pour intégrer des problématiques comme le Big Data, les objets connectés, la 5G, la blockchain. Dès lors, il serait opportun d'envisager des études plus approfondies afin de déterminer les modalités de son adaptation au contexte actuel ».*

Rédigée à l'ère de l'Internet 1.0, la Convention n'évoque en effet pas vraiment les risques de l'Internet collaboratif, que nous connaissons aujourd'hui, et encore moins ceux liés à l'expansion des nouvelles technologies, qui vont inonder le monde ces prochaines années.

« Le Big Data bouleverse le monde», poursuit Elhadji Oumar Ndiaye. Il plaide pour une adaptation des législations de sorte que le principe de finalité en matière de protection des données personnelles soit mis au clair. «Quand une structure met en place de la récupération ou de la restitution des données, il faut que la finalité du traitement soit définie pour prendre en compte le consentement de la personne ». Heureusement, souligne-t-il, certains Etats n'ont pas attendu une mise à jour de la Convention pour revisiter leurs textes nationaux, notamment sur la protection des données à caractère personnel.

La 5G, une opportunité… à encadrer

Sur cette dernière question, les opérateurs télécoms sont en première ligne. Pour autant, cela constitue-t-il une menace pour les citoyens et les Etats ?

« Je ne crois pas et c'est au législateur de définir les garde-fous, répond le spécialiste en droit. Il y a lieu de préserver la liberté d'entreprise, la circulation des données et les droits et libertés des personnes. La 5G n'est pas une menace, mais une opportunité, une aubaine, dans la mesure où les Etats mettront en place des mécanismes appropriés ».

Dans les prochaines années, les législateurs devront donc jouer aux équilibristes, afin de préserver l'intégrité des personnes, sans pour autant se priver des nouvelles technologies. Car plus celles-ci évolueront, plus les cyber-menaces se multiplieront.

Ainsi, si le support technologique change, les paradigmes, qui ont guidé à l'élaboration des législations, doivent eux-aussi être revus.

« Tout l'enjeu se situe autour de la maîtrise des données. C'est la bataille à mener. Nous ne pouvons pas ériger de barrière face l'innovation », conclut Elhadji Oumar Ndiaye.

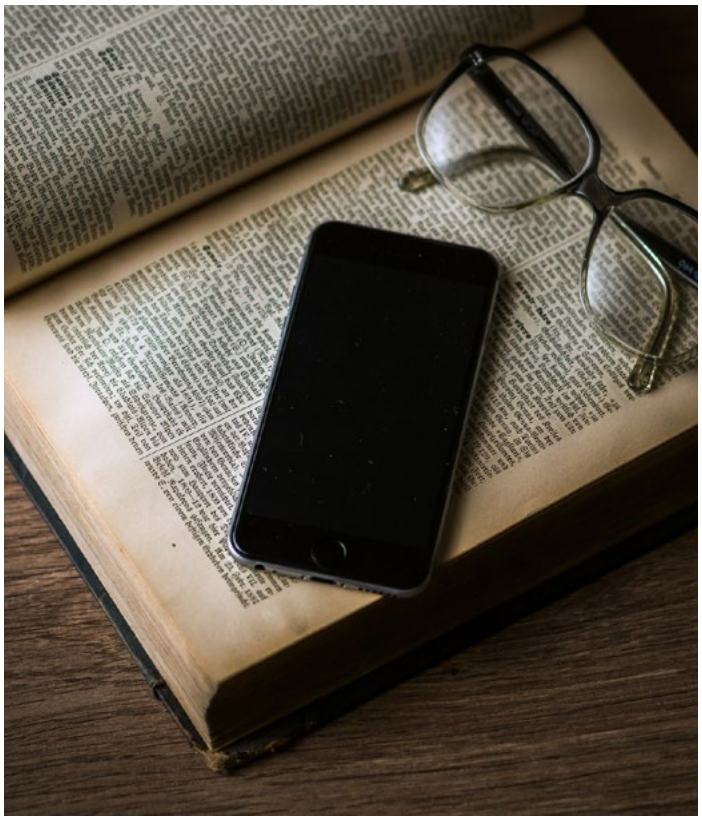
Chiffres clés

- Treize Etats africains ont signé la Convention de Malabo de 2014
- Trois l'ont ratifié, le dernier étant le Togo en 2019
- La cybercriminalité a fait perdre 3,7 MA $ à l'Afrique en 2017
- Le Nigeria a perdu 649 M $ à lui seul en 2017

COVID-19
Les cybers risques, l'autre guerre de la crise sanitaire

La crise sanitaire du Covid-19 a bouleversé les habitudes des populations du monde entier. En imposant à l'humanité la distanciation sociale, la pandémie de Coronavirus a conduit à modifier les modes de vie. Qu'il s'agisse de la consommation, des activités professionnelles, des loisirs, des urgences en tous genres, le numérique est à présent au cœur du quotidien. Malheureusement, cette forte dépendance aux solutions numériques s'est accompagnée d'une hausse des cyber-risques

Souleyman Tobias



Les facilités que procure le numérique, en cette période de crise sanitaire, s'accompagnent d'une hausse des menaces à la cybersécurité. A propos de la cybercriminalité en ces temps de crise, Thierry Delville, Associée de Price Waterhouse Cooper (PWC), déclarait le 3 avril sur France 24 que les données sont en constante évolution.

« Entre février et mars, on voit par exemple le terme Covid apparaître quatre à cinq fois plus dans les différentes campagnes de cyberattaques ». Cette déclaration dépeint bien la menace qui plane sur les usagers des solutions numériques durant la pandémie de Covid-19.

Des méthodes de hackeurs

Sur Internet, circulent de faux mails de l'OMS invitant à remplir des formulaires pour s'informer en temps réel sur le Covid-19. On trouve aussi de prétendus dispositifs d'accompagnement durant la crise sanitaire. Si ces annonces peuvent, de prime abord, sembler crédibles, il se peut que ce soient des tentatives d'hameçonnage.

Ces mails piégés permettent aux cybercriminels de voler des données privées, en se faisant passerpour une entité légitime. Mails privés ou professionnels, tout est ciblé par les hackeurs.

En cette période de télé-travail, la menace est encore plus réelle pour ceux qui collaborent avec le privé. Les pirates sont actifs sur tous les terrains. Ils peuvent même se faire passer pour des gendarmes du web. *« Nous avons remarqué une tentative d'intrusion dans votre mail, dans vos systèmes et vous invitons à cliquer sur ce lien et à suivre le processus pour vous protéger ! »* La prudence est de mise car ces mails peuvent occasionner bien des déboires aux personnes crédules. Et les obliger à payer des rançons...

Le piratage par ransomware (ou logiciel malveillant) peut se produire en cliquant sur un lien ou une pièce jointe piégée. Si une faille de sécurité existe dans une installation, alors l'attaque rançongiciel peut aussi s'exécuter à distance, en en prenant par exemple le contrôle.

Outre l'hameçonnage et le ransomware, les spams n'ont pas non plus diminué. Et polluent les mails. Ils profitent de votre inattention ! Quant aux hoax (canulars informatiques), ils surfent sur la pandémie. Dans la précipitation et sous le coup de l'émotion, l'escroc pourrait réussir sa tentative de vous faire

faire une action susceptible de compromettre votre sécurité informatique !

N'oublions pas de citer le mal du siècle, les infox ! Les fake news ont pris de l'ampleur avec la pandémie de Coronavirus. Les fausses informations chassent sur tous les terrains : santé, politique, socio-économie... elles font feux de tout bois. Et peuvent coûter cher à ceux qui les relaient.

Les cybercriminels n'ont pas réellement changé de méthode. Les modes opératoires sont quasiment restés les mêmes.

Hameçonnage, ramsonware, arnaque, harcèlement, applications piratées... tous les moyens sont utilisés pour piéger des internautes généralement mal préparés. Le nombre de victimes pourrait s'accroître d'ici à la fin de la crise sanitaire si des précautions, aussi minimes soient-elles, ne sont pas prises dès maintenant.

Contrer la cybercriminalité

Cette pandémie a pris de court ceux qui n'étaient pas réellement préparés aux usages numériques. Le télé-travail s'est, par la force des choses, imposé. Et des sociétés ont été contraintes de l'adopter ! L'impréparation constitue donc la première source de vulnérabilité. Mais ce n'est pas une fatalité.

Il est possible de se mettre à l'abri en observant des règles simples, dont certaines sont déjà connues et méritent d'être rappelées.

Il convient tout d'abord d'utiliser du matériel sûr et sécurisé. Un ordinateur ou un smartphone avec un système d'exploitation à jour, dotés d'un antivirus ou de tout autre système de détection d'intrusion, seront d'une grande utilité. Une fois cette disposition prise, on utilisera des mots de passe robustes et différents pour chaque appareil. Et s'il est presque inévitable de se connecter, il faut veiller à sécuriser sa ligne de connexion.

Une fois encore, on choisira un mot de passe privé et fort. Pour des besoins professionnels et pour des données sensibles, le recours à des méthodes de chiffrement peut être un plus.

Pour s'assurer de la fiabilité de ce que l'on ouvre (liens, fichiers, mails) ou de ce à quoi l'on répond, il est impératif de prendre son temps. Et de vérifier que l'on se connecte aux bonnes sources : sites d'information, sites officiels et applications, qui n'échappent pas au piratage.

C'est une mesure préventive qui ne prend que quelques minutes. Elle consiste à séparer les usages professionnels de ceux qui relèvent du privé. Il est recommandé de se déconnecter de tous les équipements utilisés à des fins professionnelles lorsque l'on souhaite surfer pour des raisons privées. L'idéal serait d'ailleurs d'utiliser des outils bien distincts.

La crise liée à la pandémie du Coronavirus a entrainé des situations d'urgence et de vulnérabilité à tous les niveaux. Pour autant, plutôt que de répondre par mail, par sms ou par tout autre moyen numérique à un SOS d'un contact régulier, on prendra soin de vérifier in situ et de visu la véracité de l'information. Et on ne répondra pas à une demande d'aide financière sans avoir préalablement envoyé un message de vérification à l'intéressé.

En observant des règles de prudence, en restant vigilant et en prenant son temps, on évitera les pièges des escrocs du web. Si malgré toutes ces précautions, on était victime d'un hackeur, alors il faudrait être proactif.

En changeant rapidement d'accès et en informant au plus vite vos contacts ou votre entreprise. Et, le cas échéant, en portant plainte auprès des institutions en charge de la lutte contre la cybercriminalité de votre pays ! Car, en n'agissant pas, on participe à la propagation des actes malveillants.

L'essentiel à retenir

Pour se prémunir des cyber risques :

- Se connecter à des sources fiables
- Utiliser du matériel sécurisé
- Ne répondre ou cliquer sur des mails qu'en étant sûr de la source
- Se connecter sur des sites dont l'authenticité est prouvée
- Séparer son matériel de travail de son matériel privé
- Changer rapidement ses accès si vous êtes victimes d'une cyber attaque
- Porter plainte

SENEGAL

La coopération franco-sénégalaise à l'origine de l'école de formation des élites africaines

Inaugurée le 6 novembre 2018, l'Ecole nationale de cybersécurité de Dakar va aider au renforcement, à l'échelle régionale, de la lutte contre les cyber-attaques. L'accent a été mis sur le terrorisme en ligne.

Elimane

L'Ecole nationale de cybersécurité à vocation régionale de Dakar ne manque pas d'ambitions. C'est un véritable projet cyber qui réaffirme le leadership du Sénégal dans la lutte contre la cybercriminalité.

L'école a vocation à renforcer les compétences des pays africains engagés dans la lutte contre les nouvelles menaces et en particulier, le cyber-terrorisme.

Elle est provisoirement hébergée par l'Ecole nationale d'administration (ENA) et sera prochainement installé dans la ville de Diamniadio, à une trentaine de kilomètres de Dakar.

La formation des élites du continent est au centre du projet de l'Ecole nationale à vocation régionale (ENVR). L'objectif est d'affronter les nouveaux défis qui se posent à l'ensemble des Etats de la planète. L'établissement, qui est dirigé par le commissaire Papa Gueye, ancien Chef de la division cybersécurité de la police sénégalaise, est décrit comme l'unique pôle de référence en Afrique dans le domaine cyber.

La formation de haut niveau est avant tout destinée aux policiers et aux militaires, mais s'adresse également aux civils. Les jeunes visant le monde de l'entreprise trouveront différents cursus de formations, notamment dans la lutte contre le piratage informatique, dans les cyber-patrouilles, la surveillance des réseaux sociaux ou de l'Internet.

Le programme de formation comporte des sessions sur la sécurité informatique, le renseignement numérique, la cybergouvernance et la cybercriminalité. Elles sont destinées aux forces de l'ordre, à la justice et aux entreprises privées. Un intérêt particulier est porté sur le renforcement de la coopération entre la France et l'Afrique. Le partenariat devrait, selon les autorités françaises, aboutir à la mise en place d'un pôle de référence en Afrique.

Souveraineté dans le cyberespace

« Les Sénégalais possèdent des capacités numériques avancées et nous coopérons activement avec eux dans ce domaine », confiait un proche conseiller de Jean-Yves Le Drian, ministre français de l'Europe et des Affaires Etrangères, en 2018, dans le journal *Le Monde*.

Le Chef de la diplomatie a du reste procédé à la pose de la première pierre de l'Ecole nationale de cybersécurité. A cette occasion, il a affirmé que cet établissement renforcera les capacités des Etats africains à exercer leur souveraineté dans le cyberespace.

Lors de la 5e édition du Forum international de Dakar sur la Paix et la Sécurité, le ministre français a ajouté qu'*« Internet ne peut pas être une zone de non-droit qui échappe au contrôle de nos sociétés »*.

La mise à l'abri des données stratégiques des Etats est pris très au sérieux par les concepteurs du projet, le Sénégal et la France. Tous deux sont convaincus que la coopération est le seul moyen *« de réduire les cyberattaques »*.

Un constat relayé par Sidiki Kaba, alors ministre des Affaires étrangères du Sénégal et actuellement ministre des Forces armées. Selon lui, la définition et l'acquisition de la technologie la plus appropriée permettra de protéger des informations stratégiques et favorisera le partage d'informations sur les groupes terroristes.

Coopérer pour réduire la cybercriminalité

Dès la première heure, le Sénégal et la France ont pris la mesure du danger que représentait la cybercriminalité pour les Etats. Les deux partenaires considèrent que seule la coopération peut aider à neutraliser les malfaiteurs et à prévenir les risques. Dans un communiqué rédigé *à l'occasion de l'inauguration de* l'Ecole nationale de cybersécurité de Dakar, le Quai d'Orsay a souligné que *« l'usage d'Internet pouvait servir et financer le terrorisme ou diffuser des discours extrémistes encourageant à la radicalisation »*.

Et pouvait alors constituer une menace pour la stabilité des Etats. Dans le même ordre, il a été rappelé que l'outil Internet pouvait permettre d'extorquer de l'argent ou détourner des systèmes de transfert. Et représentait un défi pour la sécurité.

« Le cyber-espace ne connaissant pas de frontière, cette criminalité peut potentiellement affecter les Etats au-delà du continent africain ».

L'école de cybersécurité fait partie d'un réseau de seize établissements présents dans dix pays. Déjà, deux Ecoles nationale à vocation régionale existent au Sénégal : l'une pour la formation de l'infanterie est située dans la région de Thiès et l'autre, dédiée aux officiers de la Gendarmerie, est implantée à Ouakam.

S'agissant de la répartition par nationalité des étudiants au sein de l'école, 30% doivent être des nationaux et 70 % proviennent des autres pays africains.

Avant que cette école ne voie le jour au Sénégal, Dakar s'était déjà imposée dans la lutte contre la cybercriminalité à travers la division spéciale de la Police nationale.

Cette dernière dépend de la Police judiciaire et est dirigée par l'actuel patron de l'Ecole nationale de cybersécurité. Papa Gueye est titulaire d'un doctorat en Droit privé et Affaires criminelles. Après des années employées à tracer et à contrer les bandits en ligne, sa nomination récompense une carrière dédiée à la lutte contre les cyber-attaques.

BÉNIN

Epitech sort sa première promotion d'experts en informatique en 2021

Le réseau d'école pour l'informatique et les nouvelles technologies (Epitech) a ouvert sa première franchise africaine au Bénin, en 2019. Elle est implantée à Sèmè City, une smart city disposant d'un écosystème propice à l'innovation et qui stimule la créativité. D'ici à fin août 2021, la première promotion d'étudiants aura achevé le cursus anglophone de trois ans basé sur une pédagogie innovante. Et qui replace l'apprenant au cœur de sa formation.

Michaël Tchokpodo

Edwin Kouassi, étudiant ivoirien, est inscrit en 2ème année à Epitech Bénin. Après l'obtention de son baccalauréat, en 2018, il a eu des difficultés à trouver une école d'informatique.

« *Je cherchais des écoles qui forment en informatique, lorsque mon père m'a parlé d'Epitech. J'ai fait des recherches sur la façon dont se déroulent l'enseignement et la vie estudiantine. Et j'ai été séduit par le fait que ce soit 100% pratique et qu'il n'y ait pas d'autres matières, comme en cours classique* », témoigne-t-il. Comme lui, une vingtaine d'autres étudiants ont opté pour la singularité de l'apprentissage à Epitech Bénin et en constituent la première promotion.

Pour les sélectionner, l'équipe d'Ouanilo Medegan Fagla, cofondateur de l'école, a misé sur les résultats du bac et a fait passer des tests d'anglais, de logique et de code basique. « *Notre sélection est drastique. Nous ne gardons que ceux qui peuvent aller jusqu'au bout des épreuves de sélection. Lors des entretiens de recrutement, nous testons les réflexes et la manière de penser de nos futurs apprenants. Ils n'ont pas besoin d'être experts en programmation ou en maths pour se présenter. Nous avons différents ateliers qui nous permettent d'évaluer leur réaction face à un problème, ainsi que leur culture générale en informatique et leur motivation.* »

Rigueur et autonomie

Dès les premiers jours, l'étudiant est confronté à la pratique et il lui est demandé de coder dans l'un des langages programmatiques les plus ardus. L'étape de la piscine est le point de départ du premier cycle à Epitech. Mais, dans ce contexte, il ne s'agit pas d'apprendre à nager.

« *Pendant quatre semaines, les journées commencent à 8h42 et finissent à 23h42. Les élèves sont régulièrement amenés à dormir sur place (l'école est ouverte 24heures/24, 7 jours/ 7). On les met en face de ce que l'on attend d'eux tout au long du cursus : un rythme de travail intensif, l'émulation entre étudiants, la rigueur et des projets exclusivement en anglais* », précise Johanne Bruffaerts, Directrice du développement à Epitech Bénin.

Tout au long du cursus, 150 projets sont soumis aux étudiants, au cours du tronc commun de formation sur l'expertise informatique.

Ce n'est qu'à partir de la 3ème année qu'ils peuvent choisir des modules de spécialisation. Durant leur formation, ils doivent faire preuve d'une très grande rigueur et d'une très forte autonomie. S'agissant des recrues à leur arrivée à Epitech, Ouanilo Medegan constate :

« *On sentait qu'elles n'étaient pas nécessairement débrouillardes. Elles n'aimaient pas déranger et subissaient leur problème au lieu d'aller vers l'équipe d'encadrement. Par ailleurs, on a trop souvent mis l'accent sur la notion de note. Or, à Epitech, ce n'est pas la note qui importe. On maîtrise tous les mécanismes pour détecter les compétences que vous activez.* »

Développer les soft skills

Pour la mise en œuvre de sa pédagogie, Epitech Bénin dispose d'un coach en développement personnel et d'un responsable pédagogique. Leur mission ? Développer chez les étudiants une capacité de résilience qu'ils peuvent mobiliser dans tout type d'environnement professionnel. Et les pousser à s'améliorer.

« *En tant que coach académique, explique Affissou Prince Amidou, Spécialiste en développement personnel, je développe les Soft Skills (compétences comportementales). Le but est de se focaliser sur les compétences*

humaines essentielles au développement de l'intelligence émotionnelle. Ces compétences vont faciliter l'apprentissage des apprenants qui sont confrontés aux exigences du milieu scolaire et professionnel. J'aide les étudiants à gérer les tensions intrapsychiques et interpsychiques qui apparaissent durant toute phase d'apprentissage intense. »

L'objectif de cette démarche est de permettre aux étudiants de puiser dans leurs ressources personnelles la force nécessaire pour résoudre les problèmes que leur poseront leurs futurs environnements professionnels. *« L'environnement de travail que nous créons au sein d'Epitech est très similaire au monde de l'entreprise. Il permet à l'étudiant d'être l'acteur principal de son processus d'apprentissage. Il choisit lui-même les projets qui l'intéressent dans le cadre de groupe de connaissances fondamentales. L'étudiant gagne ainsi en autonomie »,* atteste Emmanuel Solomo, Responsable pédagogique.

L'apprentissage par projet

La formation à Epitech Bénin se déroule à l'Agence de développement de Sèmè City, une smart city hébergeant des Start-ups innovantes et des laboratoires de recherche. L'objectif est d'implanter progressivement un écosystème favorable à l'innovation. La smart city est engagée aux côtés d'Epitech Bénin et lui apporte son soutien à travers l'accompagnement sur certains projets innovants. Grâce à son réseau de partenaires, les étudiants bénéficient de stages aussi bien au niveau local et continental qu'à l'international. Ils peuvent se confronter à des compétences étrangères. Et pourront mettre à l'épreuve l'apprentissage par projet reçu – à titre individuel ou collectif -, afin de devenir *« des professionnels experts, autonomes, rigoureux, fiables, communiquant, innovants et leaders. »*

« La méthodologie d'Epitech est très enrichissante. Cette façon de travailler nous permet de gagner en compétences et en autonomie. Il est vrai que les débuts sont difficiles, parce que nous n'y sommes, de prime abord, pas habitués. » Edwin Kouassi reconnait qu'avant son entrée à Epitech, il avait été habitué à prendre note des cours des professeurs, à copier des leçons, à les apprendre et à faire ensuite des devoirs. Pour Camélia Sama, la pédagogie est innovante car elle va à l'encontre de celle traditionnellement en usage au Bénin. *« C'est une pédagogie par projet, où l'étudiant touche du doigt ce qu'est réellement l'informatique et la réalité de la vie professionnelle. »*

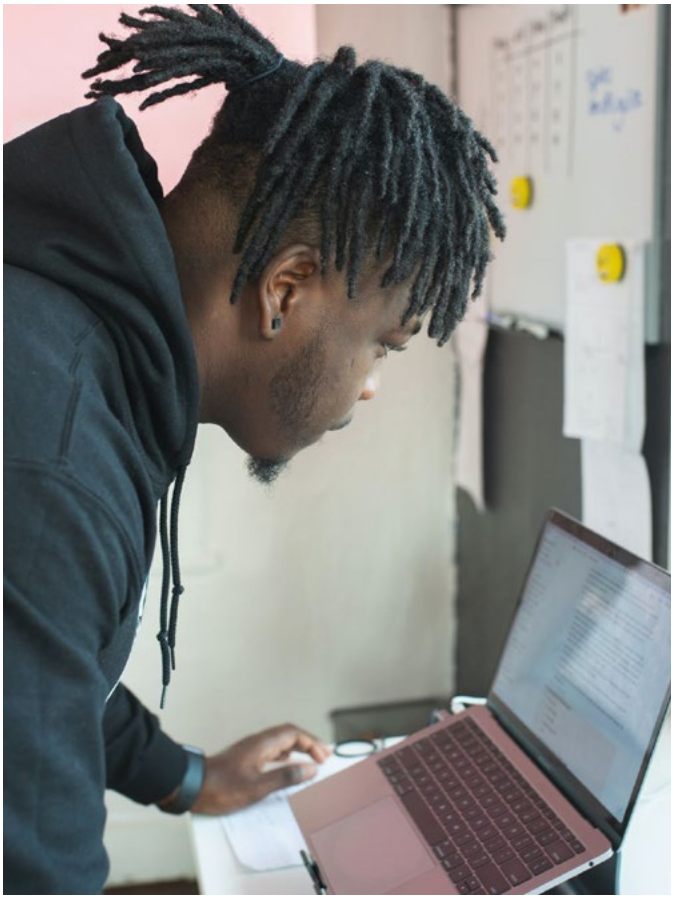
A Epitech, le niveau de formation est extrêmement élevé. Pour preuve, seuls treize étudiants ont pu franchir le cap de la première année, sur les vingt-et-un inscrits au départ. Ils obtiendront leur diplôme en 21 août 2021, avec la conviction que leur capacité d'apprendre à apprendre et à se dépasser les démarquera de leurs challengers. A cela s'ajouteront leur sens de l'autonomie, leurs nombreuses compétences techniques, leur rigueur, leur bon niveau d'anglais, leur expérience en entreprises, et celle acquise lors de challenges et de concours. *« Nous formons nos étudiants pour qu'ils soient prêts et à la hauteur quand ils finissent leur cursus »,* conclut Johanne Bruffaerts, d'Epitech Bénin.

FORMATION

Pourquoi envisager une carrière dans la cybersécurité ?

L'accélération et le développement des e-services et des systèmes d'information sont proportionnels aux risques de menaces informatiques. Dans un monde qui tend vers le tout-numérique, le vol des données à caractère personnel, la cybercriminalité et la cyberattaque rendent de plus en plus vulnérables les internautes, en quête de protection.

Michaël Tchokpodo



Selon des statistiques, chaque année, dans le monde, 80% des entreprises dotées d'un système d'information ou dont une partie des activités repose sur un système d'information déclarent être touchées par une cyberattaque. 59% d'entre elles déclarent que ces attaques ont eu un impact important sur leurs activités. Parfois, elles les ont tout bonnement stoppées. Alors qu'on évalue à 4 millions le besoin mondial d'experts en cybersécurité des entreprises, celles-ci n'en trouvent pas. Les compétences dans ce domaine manquent.

Ces chiffres, rapportés par le Capitaine Miguel Sossouhounto, Manager de l'équipe béninoise de réponse aux incidents de sécurité informatique, attestent de l'urgence à disposer de ressources humaines de qualité pour sécuriser le cyberespace, l'écosystème et les infrastructures.

« La cybersécurité est déjà un enjeu majeur pour beaucoup de secteurs : administration, industries, banque, télécommunications, services, etc. Dans un environnement de plus en plus menaçant, où la menace persiste et ne fait parfois pas de distinction avant d'attaquer, les défis liés à la sécurisation des actifs sont réels », prévient le manager du bjCSIRT. Ce Computer Security Incident Response Team (CSIRT) est le premier point de contact du Bénin en cas d'incident de sécurité informatique.

Fawaz Moussougan, spécialiste en cybersécurité, confirme. *« Souvent plus simples, moins risquées et plus efficaces, les cyberattaques sont amenées à se multiplier. Elles sont également de plus en plus sophistiquées et plus difficiles à combattre. S'en protéger est sans aucun doute l'enjeu majeur de la sécurité au XXIème siècle. Le risque n'épargne aucun type de structure, ni aucune organisation. »* Ces défis de sécurité numérique s'imposent aux citoyen, mais surtout aux entreprises et aux Etats, car des attaques informatiques peuvent à tout instant paralyser leurs infrastructures critiques. Ce procédé de déstabilisation porte atteinte à la confiance numérique.

Confiance numérique

L'instauration de la confiance numérique repose en effet sur l'humain. C'est l'un des facteurs clés qui prouve la capacité à adopter une hygiène numérique. Selon Fawaz Moussougan, Certified Ethical Hacker, cela passe par la formation et la sensibilisation des internautes à des règles, telles que : *« choisir avec soin*

ses mots de passe » ; « *séparer les usages personnels des usages professionnels* » ; « *mettre régulièrement à jour ses logiciels* » ; « *bien connaître ses utilisateurs et ses prestataires* » ; « *effectuer des sauvegardes régulières* » et « *sécuriser l'accès Wi-Fi de son entreprise* ».

Mais au niveau des infrastructures, il convient par exemple de « *maîtriser les risques d'infogérance, d'attribuer les bons droits sur les ressources sensibles du système d'information et de définir et de vérifier les règles de choix et de dimensionnement des mots de passe* ».

Il est aussi recommandé de « *disposer d'un inventaire exhaustif des comptes privilégiés et de les maintenir à jour* ».

La mise en œuvre de ces règles, au sein d'une administration ou dans un pays, ne peut néanmoins s'effectuer sans une définition préalable et sans une politique de sécurisation de l'écosystème et des actifs. A ce niveau, il s'agit de la sécurité organisationnelle, qui précède et crée, en aval, le cadre de mise en application de la sécurité technique.

Evidemment, cette politique nécessite une feuille de route, des moyens financiers, un engagement réel et la mobilisation des compétences pour sa réalisation et son suivi.

Carrière dans la cybersécurité

Face à ces exigences techniques, la tâche doit être confiée à un expert. Il peut restaurer ou garantir la cybersécurité d'un écosystème ou d'une infrastructure.

« *Envisager une carrière dans la cybersécurité est l'un des choix les plus utiles qu'un ingénieur peut actuellement faire, surtout dans les domaines de l'informatique et des télécommunications en général* », affirme Miguel Sossouhounto. Il ajoute que les compétences dans le domaine de la cybersécurité sont mondialement recherchées.

Une situation qui s'explique par le développement exponentiel des e-services et du fait de l'accélération de la transformation digitale de la société. Pour mener à bien cette riposte, plusieurs compétences interviennent dans le processus, explique le manager du bjCSIRT. A commencer par le responsable de la sécurité des systèmes d'information.

« *Il peut être appelé quand l'entreprise fait face à une crise cyber.* » Il est épaulé par le chef projet sécurité, le développeur sécurité, l'intégrateur de sécurité, l'administrateur de sécurité, l'analyste SOC et les consultants sécurité organisationnelle, technique, etc. Chacun de ces spécialistes a un savoir-faire assez distinct, mais qui est complémentaire pour la résorption d'une cyberattaque.

« *Tout le monde a besoin de protection, qu'il s'agisse d'une petite Start-up en plein essor ou d'une entreprise dont les revenus se chiffrent en milliards de dollars.La cybersécurité continue d'évoluer, tout comme le reste du monde technologique. Ce qui signifie que de nouveaux rôles vont émerger, tandis que les anciens vont progressivement évoluer pour englober de nouvelles compétences* », renchérit Fawaz Moussougan.

Sécuriser l'écosystème

En nourrissant l'ambition de faire du Bénin la plateforme des e-services en Afrique de l'Ouest, le chef de l'Etat Patrice Talon a créé, à son arrivée au pouvoir en 2016, un environnement propice à l'évolution numérique. Sa politique a favorisé la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI-Bénin). Elle est chargée de la mise en œuvre des orientations de la stratégie nationale de sécurité du numérique. Pour faciliter ses actions, le Bénin s'est doté d'un Code du numérique. Il a vocation à réprimer les infractions liées au numérique, en lien avec l'Office centrale de répression de la cybercriminalité (OCRC). La dématérialisation des services de l'Etat a par ailleurs trouvé un répondant à travers la création du portail national des services publics.

Le Bénin, qui a créé le bjCSIRT, compose avec sa jeunesse pour assurer la sécurité de son écosystème et de ses infrastructures. Cela se traduit par l'organisation, depuis 2017, du HackerLab, un concours de détection des talents en cybersécurité.

« *100% des analystes juniors du bjCSIRT sont issus de ce concours, se réjouit le Capitaine Sossouhounto. Ils font le job avec efficacité. Avec cette émulation, le Bénin découvrira certainement encore des talents beaucoup plus prometteurs. Le pays en dispose déjà. Il suffit qu'ils soient stimulés pour produire le rendement escompté.* »

BÉNIN
Face au Covid-19, l'ANSSI plus que jamais d'attaque

Si l'Agence nationale de la sécurité des systèmes d'information du Bénin s'est assurée de la sécurisation des infrastructures numériques et du cyberespace béninois avant la crise sanitaire mondiale liée au Coronavirus (Covid-19), elle est actuellement beaucoup plus sollicitée. Malgré cela, elle maintient son plan d'actions et les projets phares du secteur du numérique.

Michaël Tchokpodo

L'apparition et la confirmation des premiers cas de Covid-19 au Bénin ont drastiquement réduit les déplacements des citoyens, surtout depuis qu'un cordon sanitaire a été instauré par le Gouvernement.

Dans ce contexte, les entreprises ont recours au télé-travail pour ne pas être contraintes d'interrompre leurs activités. *« Dans le numérique, chaque fois que l'on ajoute une brique ou un nouveau processus, on étend le périmètre ou la surface d'attaque »*, fait remarquer Ouanilo Medegan Fagla, Directeur général de l'Agence nationale de la sécurité des systèmes d'information du Bénin (ANSSI-Bénin).

Ces attaques sont de plusieurs ordres : la compromission de l'ordinateur d'un employé en télé-travail, la cybercriminalité ou la cyberattaque.

Ainsi, l'ANSSI a très tôt pris les devants de cette lutte en diffusant un guide de bonnes pratiques de sécurité du télé-travailleur. Parmi les recommandations formulées aux internautes, on préconise d'*« installer des mises à jour de sécurité »*, d'*« utiliser un VPN et les méthodes d'authentification doubles prévues par l'employeur afin d'accéder de manière sécurisée aux ressources de l'entreprise »* ou encore de *« ne pas installer les applications mobiles sur le thème du Covid-19, mais plutôt de s'informer sur la crise à partir des canaux officiels. »*.

Sécurité numérique

Alors que le guide du télé-travailleur est destiné aux entreprises privées et aux particuliers, l'ANSSI œuvre également à la sécurité informatique des membres du gouvernement et de leurs infrastructures.

Au regard de cela, Ouanilo Medegan estime que le Covid-19 a au moins un bénéfice : celui d'accélérer la transformation digitale des institutions *« Tous les informaticiens ont une sorte de petite fenêtre dans laquelle ils peuvent intégrer leurs besoins et en tirer satisfaction. Le télé-travail est vrai outil pour les gens. C'est un plus en terme de transformation digitale. »*

Pour autant, l'ANSSI maintient sa feuille de route, laquelle consiste en la mise en œuvre de la stratégie nationale de sécurité numérique. Elle consiste à classifier les systèmes d'information (SI) pour en connaître les forces et les risques en présence, et en acquérir la maitrise. Les connaissances des SI permettront de finaliser les politiques de sécurité des systèmes d'information de l'Etat et leur mise en place, ainsi que celles afférentes à la protection des infrastructures critiques.

En parallèle, l'ANSSI est associée à la totalité des projets du secteur du numérique pour s'assurer qu'il n'y a aucune faille au niveau de leurs systèmes de sécurité.

Grands projets

En droite ligne avec ses prérogatives, le cyberespace béninois et les infrastructures informatiques restent la priorité de l'ANSSI. Et la mise en place du système national d'infrastructure à clé publique (PKI) est l'un de ses projets phares.

Il s'agit d'une plateforme de sécurisation de documents administratifs électroniques tels que : le passeport, la carte d'identité, les transactions, la signature, les documents et les services en ligne.

Au Bénin, cette réforme est déjà opérationnelle grâce à l'émission des cartes nationales d'identité électroniques, des passeports électroniques et de la mise en service de la plateforme www.servicepublic.bj, qui est le portail national des services publics.

En cas d'incident informatique, le premier point de contact avec les institutions de l'Etat est bjCSIRT, une équipe gouvernementale de réponse aux incidents de sécurité informatique.

Cette police du cyberespace béninois travaille en étroite collaboration avec la police républicaine et l'Office central de répression de la cybercriminalité (OCRC) pour démanteler les réseaux de cybercriminels.

AFRIQUE DU SUD
Un niveau de risque de cyberattaques inquiétant

L'année dernière, dans la plus importante ville sud-africaine, plusieurs banques, voire même les populations, ont tremblé sous la menace d'une importante cyberattaque. Quelques mois après, la cybercriminalité est toujours à la hausse et le niveau de sécurité est, selon des experts, encore aléatoire.

Aurore Bonny

« Tous vos serveurs et vos données ont été piratés. Nous avons dérobé des dizaines de sites à l'intérieur de votre ville. Nous en contrôlons l'intégralité. Nous avons également compromis tous les mots de passe et les données sensibles, telles que celles des finances et les informations personnelles sur la population ».

C'est en ces termes qu'a été rédigé le message des cybercriminels, qui se sont attaqués au portail virtuel d'e-services de la ville de Johannesburg.

Une rançon de quatre bitcoins, soit 500 000 Rand sud-africain ou 37 000 dollars a été exigée. Elle devait être versée avant le 28 octobre, à 17h00, pour que les données de la ville ne soient pas diffusées sur Internet. Les banques et la population ont connu une menace similaire au cours de la même période.

Selon les experts, il s'agissait de deux sortes d'attaques pirates. La première, un Ransomware, qui est généralement livré par email ou par phishing, était destinée à la ville.

La seconde, une attaque DDoS, était dirigée contre les sites Web et les services en ligne des banques.

Cette dernière n'implique pas de piratage ou de violation de données et donc aucune donnée client n'est en danger. Elle implique une augmentation

du trafic sur les réseaux pour accéder aux services accessibles au public. Cela peut provoquer des perturbations mineures. Chaque organisation devrait être prête à se défendre contre ces attaques typiques et courantes.

Pour gérer cette situation, la ville, confiante, a refusé de céder au chantage et a dans un premier temps fermé son site web, tout en suspendant ses e-services pour 24 heures.

Elle a misé sur l'assistance des experts en cyber sécurité pour mener une enquête, de sorte à renforcer les mesures de sécurité. Certaines banques ayant pris la même initiative ont annoncé plus tard que la situation était stabilisée.

Des spécialistes ont salué l'initiative de sauvegarde de la Ville de Johannesburg et son refus de céder au chantage.

« Lorsque les victimes paient la rançon, alors le Ramsomware offre aux criminels une belle opportunité de gagner de l'argent. Cela étant, il est toujours facile de ne pas payer de rançon lorsque ce ne sont pas vos données ou services qui sont retenus en otage », avait déclaré, à la suite de cette attaque, Tim Erlin, vice-Président de Tripwire, une entreprise américaine de cybersécurité.

Toujours des lacunes

On aurait pu croire que cet incident majeur aurait pu permettre de mobiliser d'importants moyens pour lutter contre la cybercriminalité. Mais, face à un système de sécurité qui, pour certains spécialistes, laisse à désirer, elle ne cesse d'augmenter. Pour Craig Rosewarne, Directeur général de Wolfpack Information Risk - une société sud-africaine spécialisée dans la cyber-recherche -, le niveau de risque national au regard du cyber-risques est « assez choquant ».

« D'un point de vue stratégique, notre pays est très vulnérable. J'espérais que les choses allaient s'améliorer au fil des ans avec POPI et le Cyber Crimes and Cyber Security Bill, mais ce n'est pas le cas », a-t-il déclaré.

Selon la presse locale, qui a repris son propos, l'entrepreneur constate que dans le secteur privé sud-africain, la question de la cybersécurité figure parmi les trois ou cinq principales préoccupations en entreprise.

En revanche, dans le secteur public, l'urgence et la réactivité ne seraient pas du même acabit. D'aucuns auraient plutôt tendance à s'asseoir et à attendre.

Craig Rosewarne pense que de nombreuses violations sont tues et ne sont non mentionnées hors de l'entreprise. De son point de vue, il faudrait que les informations sur le mode opératoire utilisé par les cybercriminels, pour intégrer les systèmes informatiques des organisations, soient partagées entre pairs.

Le Directeur général de Wolfpack Information Risk déplore le déficit de statistiques sur le nombre d'attaques et le manque de termes d'avertissements proactifs. Seul le secteur bancaire peut se targuer de réussir et prochainement les assurances et l'éducation.

S'agissant du manque de données statistiques, Zamani Ngidi, Responsable client de Cyber Solutions chez Aon, a expliqué à la presse sud-africaine qu'un grand nombre de personnes ignore ce qu'il en coûte à une entreprise de subir une cyber-violation. La réponse à une violation de cette nature génère a posteriori des coûts commerciaux.

« Cela peut aller de l'interruption des activités et la perte de confiance des entreprises et des clients, à la responsabilité des administrateurs et des dirigeants, jusqu'à l'atteinte à la réputation » a-t-il expliqué.

Dans un rapport sur le cyber sécurité, élaboré en 2019 par Aon South Africa, les vulnérabilités qui ont permis aux cybercriminels d'exécuter des attaques à grande échelle ont été révélées.

Il s'agit de l'accès aux données opérationnelles des appareils mobiles et périphériques, de la menace causée par la faiblesse de l'Internet des objets, mais aussi des employés qui constituent un maillon faible potentiellement exploitable par les criminels. Ces derniers se serviraient des anciens membres des services de renseignement pour effectuer leurs actes délictueux.

Un problème de logiciel obsolète peut également constituer un point d'entrée pour les cybercriminels d'Afrique du Sud.

D'après Maher Yamout, Chercheur principal en sécurité au sein de Kaspersky, 34% des ordinateurs sud-africains utilisent une version obsolète ou non prise en charge par le système d'exploitation

Microsoft Windows. Cette version non conforme présente un risque d'infection plus élevé. Le responsable du groupe russe a révélé que 5% du marché des systèmes d'exploitation non pris en charge sont constitués d'utilisateurs de Windows XP, un support qui a pris fin en 2014.

« Une organisation peut disposer des meilleures solutions de cyber sécurité disponibles sur le marché, il suffit d'un appareil avec un système d'exploitation obsolète pour que toute l'entreprise soit compromise », a-t-il expliqué.

Force est de constater que le tableau statistique de la cybersécurité en Afrique du Sud n'est pas très rassurant. Kaspersky a relevé, qu'en 2019, les attaques de logiciels malveillants ont augmenté de 22%, comparativement au premier trimestre de l'année précédente.

Quant aux détections de logiciels, elles ont progressé de 8%, toujours à même époque, tandis que les logiciels malveillants mobiles enregistraient une augmentation de plus de 17%.

Selon des données fournies par Amin Hasbini, Responsable de la recherche et de l'analyse mondiale pour Kaspersky au Moyen-Orient, en Turquie et en Afrique, chaque jour, on dénombre environ 13 842 cyberattaques en Afrique du Sud, soit 577 tentatives d'attaque toutes les heures, équivalentes à 9 par seconde.

Pire avec le Covid-19

L'expansion du Coronavirus complique encore davantage la situation. Ces dernières semaines les experts alertent. Avec le confinement, le télé-travail se développe, en même temps que l'usage des appareils connectés à domicile.

Et avec moins de sécurité, parfois même sans aucune sécurité. Quoi de mieux pour les bandits de l'ère numérique ? Du 15 au 21 mars, Kaspersky a relevé jusqu'à 310 000 attaques pirates d'appareils, soit plus de la moyenne hebdomadaire, qui se situait autour de 20 à 30 0000 attaques.

Dans une récente interview, Martin Butler, Maître de conférences en Transformation numérique à l'Université de Stellenbosch Business School (USB), recommande aux entreprises de s'assurer que leurs employés, travaillant à distance, effectuent *« l'équivalent numérique du lavage des mains, du port des masques faciaux, de la distance physique et de la décontamination »*.

Pour lui, il ne suffit pas de garantir que les politiques de l'entreprise soient appliquées sur l'ordinateur portable, si celui mis à disposition par l'employeur - et utilisé pour le télé-travail - partage un réseau domestique avec plusieurs autres appareils, tels que des téléphones portables.

Cette période de télé-travail est d'après lui le moment idéal pour qu'un utilisateur anxieux et peu averti en technologie, qui souhaite connaître les dernières nouvelles et informations sur le Covid-19, active un lien vers un logiciel malveillant.

« Une action mal menée peut faciliter l'accès à un logiciel de rançon, lequel peut pénétrer dans les défenses des entreprises à partir d'emplacements distants ».

Chiffres clés

- 34% des ordinateurs sud-africains utilisent une version obsolète - ou non prise en charge - du système d'exploitation Microsoft Windows. Ils peuvent présenter un risque d'infection plus élevé à l'insu des utilisateurs.
- Au premier trimestre de l'année 2019, l'Afrique du Sud a vu les attaques de logiciels malveillants augmenter de 22% par rapport à l'année précédente.
- Chaque jour, on dénombre 13 842 cyberattaques, soit 577 tentatives d'attaque toutes les heures, équivalentes à 9 par seconde.
- Pendant la période de confinement, du 15 au 21 mars, Kaspersky a relevé jusqu'à 310 000 attaques pirates d'appareils, soit plus de la moyenne hebdomadaire, qui se situait autour de 20 à 30 0000 attaques.

AFRIQUE
« La cybersécurité n'est plus une option »

Ali El Azzouzi est fondateur et directeur général de DATAPROTECT, une entreprise spécialisée en sécurité de l'information. Elle fournit des services de supervision de la sécurité des systèmes d'information auprès de nombreux clients, tels que les banques, les opérateurs télécoms et les assurances, au Maroc et en Afrique. PourCIO Mag, le responsable analyse les enjeux de la question cybersécuritaire en Afrique.

Ali El Azzouzi
Fondateur de DATAPROTECT

La cybersécurité est devenue une question de bonne gouvernance. Une institution qui subit une attaque saisit immédiatement son management.

Si aujourd'hui la cybersécurité est systématiquement inscrite à l'agenda des conseils d'administration de grandes structures, c'est pour une bonne raison. Et ce n'est plus une option. La cybersécurité est un « must ». Nous avons mené de nombreuses études de terrain en Afrique. Et en déduisons à chaque fois les mêmes enjeux.

1. Le partage de l'information

Dans le domaine de la cybersécurité, le partage d'information ne relève pas du simple « networking ». Il s'apparente plutôt à un outil pour prévenir les incidents de cybersécurité. La cybersécurité ne peut pas être assurée par une équipe de deux ou trois personnes, aussi talentueuse soit-elle, mais par la création, au sein de la communauté financière, d'échanges constants et systématiques autour des meilleures pratiques. L'information partagée porte aussi bien sur l'existence de la menace elle-même, que sur les indicateurs techniques (caractéristiques de la menace) et sur les données opérationnelles (nature de l'attaque et nature de la cible, contre-mesures déployées, etc.). C'est cet ensemble de processus qu'il convient de formaliser de manière détaillée. À cette fin, il est indispensable de créer un cadre de concertation.

Ce partage est généralement volontaire, mais encore faut-il créer le cadre propice au plan législatif, réglementaire et financier. Le partage peut aussi être obligatoire. La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) tient alors un rôle de première importance. Sa position transnationale fait d'elle un acteur central du partage de l'information.

2. Le besoin de ressources

A l'international, l'effectif d'ingénieurs en cybersécurité est estimé à plus de trois millions. En Afrique, peu de ressources formées localement sont spécialisées en cybersécurité. C'est ce explique l'hésitation du continent à donner suite aux nombreux appels des multinationales en Europe, au Moyen-Orient et en Amérique du Nord. La fuite des cerveaux dans ce domaine est massive.

Il est important de promouvoir les formations spécialisées en cybersécurité pour combler ce vide.

3. Les enjeux législatifs et réglementaires

La cybercriminalité se répand d'autant plus vite que le cadre législatif et réglementaire de la plupart des pays d'Afrique est inadapté. Et, quand il existe, il est mal appliqué. En effet, il ne suffit pas d'avoir des lois et de disposer de l'arsenal juridique qui existe en Europe. Il faut appliquer ces lois et c'est ce qui pose problème dans de nombreux pays africains.

L'Afrique, plus exposée que le reste du monde

Pour certains analystes, l'Afrique est un « paradis cybercriminel ». De nombreux pays africains sont dans le Top 10 des pays les plus actifs en matière de cybercriminalité. Les recettes annuelles se chiffrent en milliards de dollars. L'absence de barrières à l'entrée, le faible risque d'arrestation du fait de l'état embryonnaire de l'arsenal répressif, l'attractivité sur le plan financier... Tout cela encourage de nombreuses personnes malveillantes à se lancer dans des activités cybercriminelles en Afrique. Par ailleurs, le faible niveau de sécurité de nombreuses entreprises attire la convoitise de la communauté cybercriminelle mondiale. Dans plusieurs secteurs névralgiques, il est en effet plus facile de cibler des entreprises en Afrique que dans le reste du monde. De ce point de vue, le continent demeure plus exposé aux risques cybernétiques que le reste du monde.

Le management de l'organisation ne peut faire abstraction de l'existence de ces risques et il doit prendre ses responsabilités. Pour y parvenir, il est important de cerner les trois dimensions de la sécurité. A savoir :

1. La dimension technologique

Cela consiste à mettre en place les dispositifs de sécurité permettant d'assurer la prévention et la détection de tout évènement indésirable susceptible de porter préjudice à la sécurité de l'information.

2. La dimension organisationnelle

Il s'agit d'élaborer la politique de sécurité de l'information et de la décliner en un ensemble de processus, de procédures et d'instructions, de sorte à formaliser les actes et à organiser la lutte contre la cybercriminalité.

3. La dimension humaine

Les deux précédentes dimensions n'auront aucun sens sans la mise en place d'une stratégie visant à sensibiliser l'ensemble du personnel autour des risques cybernétiques. Et sur les enjeux cyber. Former, éduquer et sensibiliser constituent la pierre angulaire de toute stratégie de cybersécurité.

Le Covid-19, facteur de risques aggravés

Le contexte d'incertitude liée à la pandémie de Covid-19 est très favorable à la recrudescence des cyberattaques. En effet, si des personnes malveillantes pratiquant le ransomware et sans aucune scrupule, osent attaquer des hôpitaux, un peu partout dans le monde, en cherchant à tirer profit de la crise sanitaire actuelle, les particuliers et les entreprises ne peuvent être épargnés. Au contraire, ils sont la cible de toutes sortes d'attaques.

Par ailleurs, les organisations cherchent à maintenir leur activité en permettant à leurs employés d'opter pour le télé-travail. De nouveaux flux sont accessibles depuis l'extérieur et offrent la possibilité d'accéder aux ressources de l'organisation. De l'hameçonnage personnalisé jusqu'au ransomware, en passant par l'escroquerie en ligne, l'usurpation d'identité de marque, la compromission des courriers électroniques professionnels, l'arnaque au président et l'exécution de faux ordre de virements... Toutes les méthodes basées notamment sur les techniques d'ingénierie sociale ont, dans le contexte actuel, trouvé un terrain fertile pour une meilleure propagation des attaques. Si ces techniques ciblent davantage les particuliers et les télé-travailleurs, d'autres techniques plus sophistiquées, et qui profitent de la confusion engendrée par Covid-19, visent carrément des Etats.

Le SOC DATAPROTECT, qui supervise une soixantaine de grands comptes dont de nombreuses banques africaines, nous permet de disposer d'une très riche base de connaissances des « Uses Cases ». A titre d'exemple, depuis le mois de mars, nous avons recensé, à travers notre SOC, qui rappelons-le supervise plus de 300 000 événements par seconde, quatre fois plus d'attaques que l'année passée à la même période. C'est une situation qui ne nous surprend pas compte tenu de la situation actuelle, une situation inédite.

CÔTE D'IVOIRE
La fraude au portefeuille électronique, une cyber-escroquerie redoutable

Alors que les entreprises se digitalisent, les risques de fraudes, de cyber-escroqueries et de cyber-attaques ne cessent de croître. Les services fournis sont en effet de plus en plus virtuels et la capacité de nuisance des cybers délinquants s'accentue. La Côte d'Ivoire ne fait pas exception. Comme d'autres, elle est impactée par la cybercriminalité.

Anselme AKEKO

« *Tout commence par un message qui vous informe que vous avez reçu un transfert d'argent. Quelques minutes après, vous recevez l'appel d'un inconnu vous indiquant qu'il s'agit d'une erreur. Ensuite, votre interlocuteur peut vous demander deux choses : soit de bien vouloir restituer la moitié de l'argent ; soit de consulter votre solde pour vérification. Dans les deux cas, quand vous vous exécutez, votre compte est automatiquement débité, car vous avez effectué, à votre insu, un transfert en attente initié par votre interlocuteur.* »

Sur sa page Facebook, la Plateforme de lutte contre la cybercriminalité (PLCC) explique le mode de fonctionnement de la fraude sur le porte-monnaie électronique. En matière d'infractions spécifiques aux TIC, c'est la tendance actuelle. Elle est redoutable car elle bien ficelée et est amenée par une technique d'ingénierie sociale. Officiellement, 538 cas ont été enregistrés en 2018, soit une augmentation de 15,80 % par rapport à 2017. Le chef de la PLCC explique cette hausse par la « *trop grande confiance* » des utilisateurs pour le monde virtuel.

« *A l'instar des autres pays de l'Afrique subsaharienne, les services de Mobile money sont nouveaux pour les Ivoiriens. D'ordinaire, les opérations de dépôt et de retrait d'argent se réalisent dans un établissement financier. Aujourd'hui, la vulgarisation du digital a rendu possible ces transactions par la téléphonie mobile et cela favorise les risques de fraude. Par ignorance, les utilisateurs participent plus ou moins à l'exécution de l'infraction, en communiquant des informations personnelles* », explique Fofana Mamadou, Commissaire de police. L'analphabétisme constitue un facteur aggravant. « *Une touche appuyée par erreur sur un téléphone portable peut conduire à un désastre* », fait remarquer le patron de la PLCC. Il exhorte les opérateurs télécoms à accentuer la sensibilisation en direction de toutes les couches de la population, notamment dans les langues locales. Le commissaire Fofana se félicite de cette collaboration et pense que la sensibilisation réduira la probabilité de fraudes sur le porte-monnaie électronique.

Assainir le cyber-espace

En Côte d'Ivoire, la création de la Plateforme de lutte contre la cybercriminalité procède d'un accord de partenariat entre l'Autorité de régulation des télécommunications de Côte d'Ivoire (ARTCI) et la Direction générale de la police nationale (DGPN). L'ARTCI est représentée au sein de la PLCC par le Centre ivoirien de réponses aux incidents informatiques (CI-Cert). Ce dernier assure une assistance technique aux entreprises et une veille technologique en matière de sécurité de l'information. La DGPN a pour référent la Direction de l'informatique et des traces technologiques (DITT), qui est la direction centrale de la Police scientifique. La DITT est chargée de la cybercriminalité et du soutien technologique aux investigations. Un accord, renouvelable tous les trois ans, a été signé entre l'ARTCI et la DGPN, dans le but d'assainir le cyber-espace national.

Ces dernières années, la Côte d'Ivoire a fait l'objet de nombreuses cyber-attaques. Les dommages financiers ont atteint 5,5 milliards FCFA en 2018, contre 3 milliards l'année précédente. Le CI-Cert a notifié, aux parties prenantes impactées, que plus de 68 000

vulnérabilités avaient été comptabilisées, contre 48 350 en 2017. Soit une hausse d'environ 42%[1]. Outre la fraude sur le porte-monnaie électronique (18,81 %), les infractions essentielles auxquelles sont confrontés les agents de la PLCC sont les suivantes : utilisation frauduleuse d'élément d'identification de personnes physiques ou morales (14,23 %) ; diffusions de contenus illicites (13,08 %) ; publications d'images à caractère sexuel (10,73 %) et vols de données informatiques (1,18 %).

Prolifération des fraudes

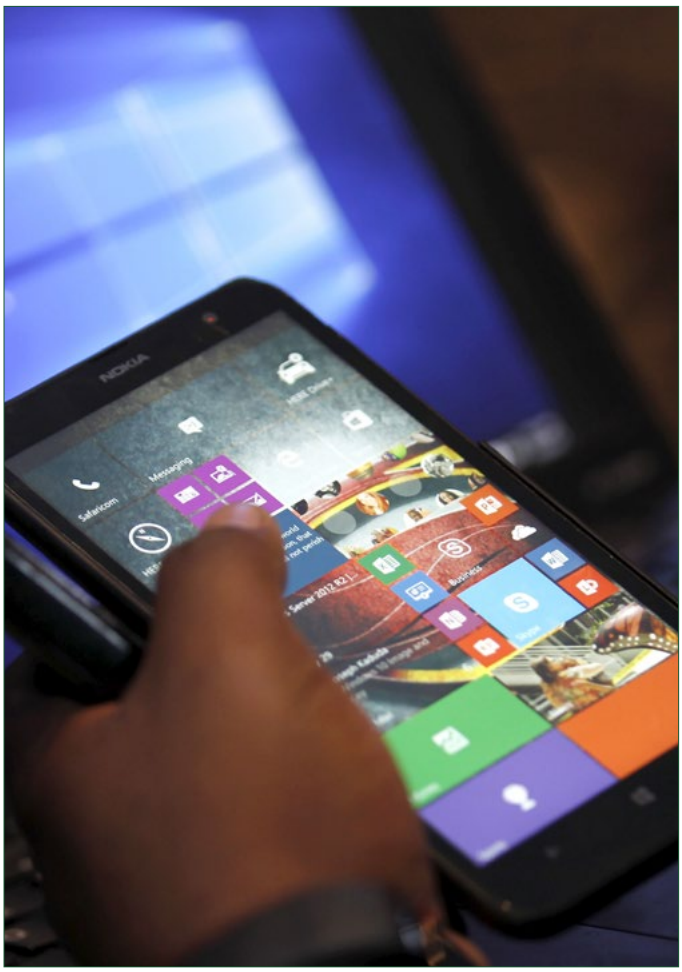
Le montant total des préjudices financiers liés aux actes de cybercriminalité, qui ont été perpétrés depuis la Côte d'Ivoire en direction de la France, du Canada, de la Suisse et de la Belgique, ce montant cumulait à 1,128 milliard FCFA en 2015. Ce qui équivaut à une augmentation de 40 %. En 2018, 2 667 plaintes ont été enregistrées par la PLCC (93,25 %). Elles sont le fait de personnes résidant en Côte d'Ivoire. La France suit avec 38 plaintes, puis le Burkina Faso (32) et le Mali (11). Pour le commissaire Fofana Mamadou, cette tendance s'explique par la prolifération des fraudes sur la transaction électronique, y compris celles sur le porte-monnaie électronique. *« Aujourd'hui, les cybers délinquants parviennent à réaliser des prises de contrôle à distance, ce qui n'était pas le cas par le passé, où il s'agissait plus d'infractions classiques favorisées par les TIC »*, commente le patron de la PLCC.

Pays d'origine des victimes	Préjudice financier en FCFA	%
Côte d'Ivoire	4 940 154 369	88,29
France	273 929 712	4,90
Liban	7 517 241	0,13
Burkina Faso	47 344 168	0,85
Espagne	3 930 000	0,07

Tableau des préjudices financiers par pays d'origine des victimes. (PLCC)

Coopération avec les multinationales de l'Internet

La capacité de nuisance des cybers délinquants s'est donc développée. Comment, dans ces conditions, la coopération peut-elle en limiter les conséquences ? Sur les bords de la lagune Ebrié, la montée significative des crimes en ligne a déjà nécessité des mesures urgentes. A commencer par le renforcement du cadre de coopération avec l'ensemble des acteurs. Mais, les multinationales de l'Internet - dont Facebook, perçu par Fofana Mamadou comme *« l'espace de commission d'infractions par excellence »* - ne sont pas forcément partie prenantes. Selon lui, l'entreprise de droit américain ne répond pas aux injonctions du procureur de la République et obstrue les enquêtes. La solution pourrait alors venir de la ratification du Traité de Budapest. Cette convention, qui favorise la coopération internationale, définit une politique pénale commune. Elle vise à faciliter la détection, l'enquête et la poursuite des comportements qui iraient à l'encontre d'autrui. Ou de ceux qui utiliseraient à mauvais escient la confidentialité, l'intégrité et la disponibilité des systèmes informatiques, réseaux et données[2].



1 Rapport CI-Cert 2018

2 Convention du Conseil de l'Europe sur la cybercriminalité - Convention de Budapest - ECPAT International

CORONAVIRUS
Attention au phishing

• De nouvelles campagnes de phishing se font passer pour l'OMS et des plateformes de conférence populaires pour dérober des informations sensibles

• Check Point a enregistré 192 000 cyberattaques liées au Coronavirus par semaine au cours des trois dernières semaines, soit une augmentation de 30 % par rapport aux semaines précédentes

• Au cours des trois dernières semaines, près de 20 000 nouveaux domaines liés au Coronavirus ont été enregistrés : 17 % d'entre eux sont malveillants ou suspects

COMMUNIQUÉ DE PRESSE

Tandis que nous essayons tous de nous habituer à la « nouvelle normalité » de la pandémie de Covid-19 dans nos vies professionnelles et personnelles, cette année a été une période d'opportunités sans précédent pour les cybercriminels. La réponse mondiale à la pandémie, et notre désir d'obtenir des informations récentes sur ce sujet, ont décuplé les activités des criminels et des pirates, et leur utilisation des emails de phishing et des faux sites web.

Au point qu'Interpol et Europol ont émis des mises en garde contre les pics d'escroqueries liées à Covid-19. À la mi-avril, Google a indiqué qu'en une semaine seulement, plus de 18 millions d'emails malveillants et d'emails de phishing liés aux escroqueries sur Covid-19 ont été envoyés quotidiennement via Gmail. Cela s'ajoute aux 240 millions de messages de spam quotidiens sur Covid-19 détectés par Google.

Pourquoi les criminels comptent-ils autant sur les emails de phishing pour lancer des attaques ? La réponse est simple : parce que cela fonctionne. Le rapport d'enquête de Verizon sur les fuites de données en 2019 indique que 32 % des fuites de données dans les entreprises commencent par des emails de phishing. Le phishing est également associé à 78 % des incidents de cyberespionnage. Il n'est donc pas surprenant que les criminels continuent d'essayer d'inciter les utilisateurs à leur révéler des informations sensibles, en profitant de l'intérêt suscité par la pandémie et en se faisant passer pour des organisations et des sociétés bien connues telles que l'Organisation mondiale de la santé (OMS), Zoom, Microsoft ou Google.

Qui essaie de m'atteindre ?

Par exemple, des cybercriminels ont récemment envoyé des emails malveillants en se faisant passer pour l'OMS à partir du domaine « who.int » avec pour objet « Lettre urgente de l'OMS : Résultats des premiers essais d'un vaccin Covid-19 sur des humains ». Les emails contenaient un fichier nommé « xerox_scan_covid-19_urgent information letter.xlxs.exe » avec le logiciel malveillant Agent Tesla. Les victimes qui ont cliqué sur le fichier ont déclencher le téléchargement du logiciel malveillant.

Nous avons également trouvé deux exemples d'emails d'extorsion prétendument envoyés par les Nations Unies et l'OMS demandant que des fonds soient envoyés à plusieurs portefeuilles de bitcoins compromis, comme illustré ci-dessous :

From: World Health Organization (srebba@ladrome.frr)

Subject: COVID-19 - Donations Needed

Body: We are all affected by the growing COVID-19 pandemic. It's an unprecedented health challenge and we know people and organizations everywhere want to help. The World Health Organization is leading and coordinating the global effort, supporting countries to prevent, detect and respond to the pandemic. The greatest need right now is the help ensure all countries are prepared, especially those with the weakest health systems. Donations support our work to ensure patients get the care they need and front-line workers get essential supplies. Now you can help by donating any amount with the help of BITCOIN NETWORK. DONATE NOW WITH Bitcoin Payment. World Health Organization Bitcoin address (BTC Wallet) for donations is: 15f7eGQt2CLJJB86jt5whrZQ5RRERCT574 Your contribution will matter! Bitcoin Wallet: 15f7eGQt2CLJJB86jt5whrZQ5RRERCT574 World Health Organization.

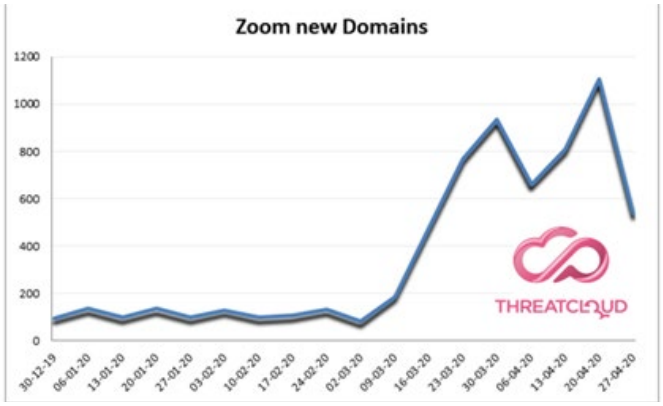
From: UNITED NATIONS (scan@falk-benelux.local)

Subject: [EXT]UNITED NATIONS COVID-19 SOLIDARITY FUND

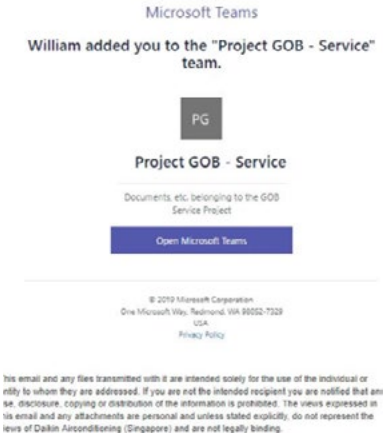
Body: Sir/Madam The United Nations Foundation and the Swiss Philanthropy Foundation have initiated this secure solidarity fund to support WHO and other partners in a massive effort to help countries affected by the Covid-19 pandemic; prevent, detect, and manage the novel corona virus. Our major aim is to concentrate in assisting those who need intensive care response hence the need for the donations to save as many lives, as possible. The Covid-19 Solidarity Response Fund is seeking your help to raise funds. This Solidarity Response Fund is a secure way for individuals, philanthropies and businesses organizations to contribute to the WHO-led effort to respond to the pandemic. We will greatly appreciate your donation through the bitcoin wallet Address below; 3P3Nt5DYMzeSYdwSmfFYx8Y7CHiBRxgQBf Any amount donated from as little as one dollar will go a long way to save lives. The fund will enable us to: Send essential supplies such as personal protective equipment to front line health workers; Enable all countries to track and detect the disease by boosting laboratory capacity through training and equipment; Ensure health workers and communities everywhere have access to the latest science-based information to protect themselves; Prevent infection and care for those in need. SUPPORT THE COVID-19 FUND We are all affected by the growing COVID-19 outbreak. It's an unprecedented health challenge and we know people and organizations everywhere want to help. The World Health Organization (WHO) is leading and coordinating the global effort, supporting countries to prevent, detect, and respond to the outbreak. Thank you, Ghada Fathi Waly Director-General/Executive Director

Usurpation de l'identité des applications de vidéoconférence

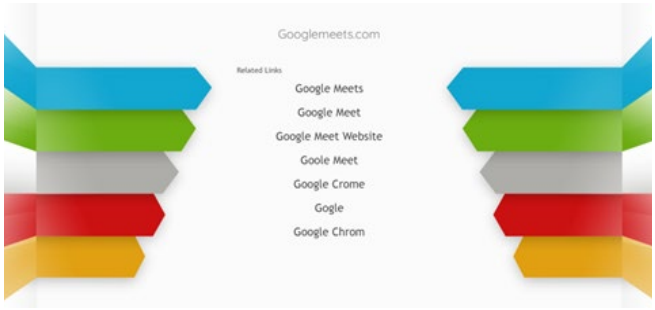
Comme le travail à domicile est désormais la norme pour une majorité de personnes pendant la pandémie, nous avons déjà signalé que des cybercriminels utilisaient de faux domaines Zoom pour leurs activités de phishing. Au cours des trois dernières semaines, 2 449 nouveaux domaines liés à Zoom ont été enregistrés. 1,5 % de ces domaines sont malveillants (32) et 13 % sont suspects (320). Depuis janvier 2020, 6 576 domaines liés à Zoom ont été enregistrés dans le monde entier.



Zoom n'est pas la seule plateforme dont les cybercriminels essaient de détourner l'identité. Microsoft Teams et Google Meet ont également été utilisées pour attirer des victimes. Récemment, des utilisateurs ont été victimes d'emails de phishing dont le sujet était « Vous avez été ajouté à une équipe dans Microsoft Teams ». Ces emails contenaient une URL malveillante («http://login/.microsoftonline.com-common-oauth2eezylnrb/.medyacam/.com/common/oauth2/ »), provoquant le téléchargement de logiciels malveillants sur les ordinateurs des victimes lorsqu'elles cliquaient sur l'icône « Ouvrir Microsoft Teams » menant à cette URL. Le lien réel menant à Microsoft Teams est « https://teams.microsoft.com/l/team ».



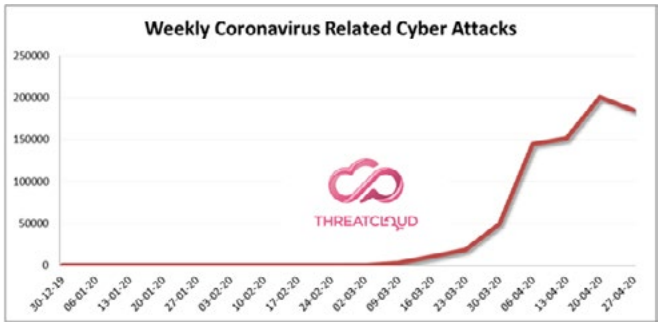
Il existe également de faux domaines Google Meets, tels que Googelmeets[.]com enregistré le 27 avril 2020. Bien entendu, le lien ne conduit pas les victimes à un véritable site web Google.



Augmentation du volume de cyberattaques liées au Coronavirus

Au cours des trois dernières semaines, 192 000 attaques liées au Coronavirus se sont produites par semaine, soit une augmentation de 30 % par rapport aux semaines précédentes. Nous définissons comme étant des attaques liées aux Coronavirus celles qui impliquent

- *Des sites web ayant pour domaine « corona » ou « covid »*
- *Des fichiers contenant « Corona » dans leur nom*
- *Des fichiers diffusés par des emails ayant pour sujet le Coronavirus*

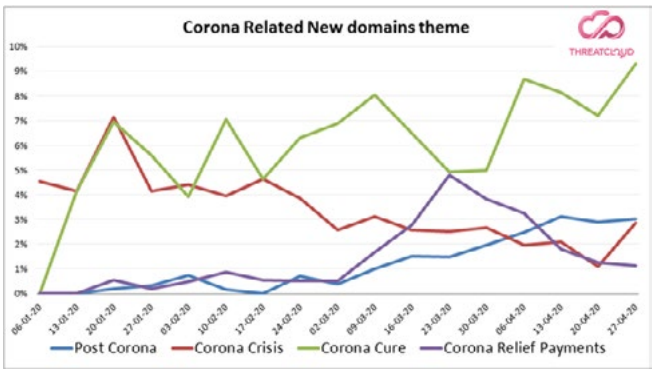


Le graphique représente toutes les attaques liées au Coronavirus, détectées par les technologies de Check Point de prévention des menaces sur les réseaux, les postes de travail et les appareils mobiles, stockées et analysées dans ThreatCloud, la base de données d'intelligence sur les menaces la plus puissante au monde.

Domaines liés au Coronavirus

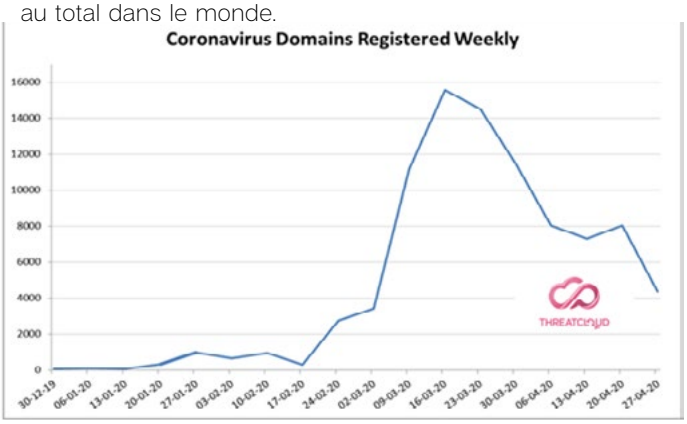
En examinant les nouveaux domaines enregistrés liés au Coronavirus, nous avons constaté qu'ils étaient une représentation fidèle des différentes étapes de la pandémie dans le monde.

- Au début de l'épidémie, les domaines comportant des cartes (les zones géographiques ayant connu une augmentation des cas de Coronavirus) étaient très courants, ainsi que les domaines liés aux symptômes du Coronavirus.
- Vers la fin du mois de mars, l'accent a été mis sur les mesures d'aide financières associées aux plans de relance économique mis en œuvre par différents pays.
- Depuis que certains pays ont commencé à assouplir les restrictions et planifier le retour à une vie normale, les domaines liés à la vie après le Coronavirus sont devenus plus courants, ainsi que les domaines concernant une éventuelle seconde vague du virus.
- Pendant toute la durée de la pandémie, les domaines liés aux kits de tests et aux vaccins sont restés très courants, avec de légères augmentations au fil du temps.



Comme nous l'avons déjà signalé, depuis la mi-février, nous avons constaté une augmentation du nombre de domaines enregistrés sur le thème du Coronavirus. Au cours des trois dernières semaines, 19 749 nouveaux domaines liés au Coronavirus ont été enregistrés. 2 % de ces domaines sont malveillants (354) et 15 % sont suspects (2 961).

Jusqu'à présent depuis le début de l'épidémie, 90 284 nouveaux domaines liés au Coronavirus ont été enregistrés au total dans le monde.



Pour se protéger des attaques de phishing liées au Coronavirus

Pour qu'une attaque de phishing soit efficace, elle doit tromper les utilisateurs. Méfiez-vous de tout email ou de toute communication provenant d'une marque ou d'une organisation connue vous demandant de cliquer sur un lien ou d'ouvrir un document joint, même si cela paraît officiel.

Un email légitime ne devrait jamais vous demander d'effectuer ces actions. Voici cinq règles d'or pour vous aider à protéger vos données :

1. Méfiez-vous des noms de domaine sosies, des fautes d'orthographe dans les emails et les sites web, et des expéditeurs d'emails inconnus.

2. Prenez garde aux fichiers reçus par email d'expéditeurs inconnus, surtout s'ils vous incitent à faire une certaine action que vous ne feriez pas habituellement.

3. Vérifiez que vous faites vos achats auprès d'une source authentique. NE cliquez PAS directement sur des liens de promotion dans des emails.
Recherchez plutôt le détaillant souhaité sur Google, puis cliquez sur le lien figurant sur la page des résultats de Google.

4. Attention aux offres « spéciales ». « Un remède exclusif contre le Coronavirus pour 150 euros » n'est généralement pas une opportunité d'achat fiable ou digne de confiance.
À l'heure actuelle, il n'existe pas de remède contre le Coronavirus et même s'il en existait un, il ne vous serait certainement pas proposé par email.

5. Veillez à ne pas réutiliser les mêmes mots de passe entre différentes applications et différents comptes.

Les entreprises devraient combattre les attaques zero-day avec une cyberarchitecture complète de bout en bout, capable de bloquer les sites de phishing et fournir des alertes en temps réel sur la réutilisation des mots de passe.

Check Point Infinity est efficace car elle combine deux ingrédients essentiels : une convergence totale sur toutes les surfaces d'attaque et tous les vecteurs d'attaque, et une prévention avancée capable de lutter contre les attaques de phishing et de prise de contrôle de compte les plus sophistiquées.

POLARIS
SECURE TECHNOLOGIES

POLARIS SECURE TECHNOLOGIES

Fondée en 2010, Polaris ST est une société de conseil spécialisée dans la sécurité des systèmes d'information. Elle est présente en France et en Afrique. Polaris ST accompagne ses clients dans tous leurs projets de sécurité informatique avec une approche globale à travers ses trois offres de services : Audit, Conseil et Formation, dans le but de leur garantir une très bonne maîtrise de la sécurité de leurs systèmes d'information.

Polaris Secure Technologies, votre partenaire en cybersécurité !

Audit

- Diagnostic SSI
- Audit de certification
- Audit d'architecture & technique
- Pentest

Conseil

- Gouvernance
- Risk Management
- Gestion de la conformité
- Expertise technique
- Résilience

Formation

- Catalogue renouvelé
- Stages pratiques
- Séminaires
- Préparation aux certifications
- Parcours sur mesure

Fondateur et CEO de Polaris ST, **Malick Fall** a débuté sa carrière dans la sécurité des systèmes d'information en 2004. Au cours de ses nombreuses missions, Il a eu à intervenir sur des domaines majeurs : de la conception de solutions de sécurité open source à la Gouvernance et Management des risques en passant par l'expertise technique, l'exploitation et l'administration d'équipements de sécurité.

Cette diversité d'expertise lui permet d'assurer des missions à forte valeur ajoutée de conseil, d'audit et des sessions de formation dans différentes organisations.

contact@polaris-st.com **www.polaris-st.com** **+33 4 78 74 50 80 / +33 7 86 00 47 79**

« Intégrer plus en amont les critères de cybersécurité »

Michel Van Den Berghe

CEO Orange Cyberdéfense

CIO Mag : Comment les opérateurs télécoms doivent-ils protéger les données des citoyens et des entreprises ? Que mettez-vous en place dans ce domaine ?

Michel Van Den Berghe : Orange a choisi de faire de la cybersécurité un axe majeur de son activité. C'est un des domaines prioritaires du plan stratégique ENGAGE 2025, lequel fixe les perspectives du Groupe pour les cinq prochaines années. Aujourd'hui, nous regroupons plus de 2000 experts en sécurité numérique à travers le monde.

Nos clients, chez Orange Cyberdéfense, sont essentiellement des entreprises, des administrations et des collectivités locales. Ils bénéficient des services complets que nous leur proposons. A savoir : l'audit de sécurité, la détection des menaces et des interventions en urgence en cas de cyberattaque avérée. Nos équipes, positionnées à l'international, peuvent intervenir à tout moment aux quatre coins du globe pour faire face aux fréquentes menaces informatiques.

Avec l'introduction des nouvelles technologies (IOT, 5G), les risques sont-ils plus élevés ? Comment, dans ces conditions, protéger les utilisateurs ?

Naturellement, le risque numérique croît avec le développement des technologies de l'information. C'est la raison pour laquelle il faut intégrer, plus en amont, les critères de cybersécurité. Comment ? En établissant une cartographie et en évaluant les actifs. En établissant une politique pour gérer les accès des utilisateurs du système d'information et en disposant d'outils de détection, de sorte à repérer les comportements inhabituels ou anormaux. Et enfin, en étant en mesure de s'appuyer sur des équipes pour obtenir des réponses à incidents en cas d'intrusion ou de dysfonctionnement. Souvent, les industriels qui fabriquent les objets connectés (capteurs, automates...) délaissent la sécurisation de ceux-ci. Cela peut être sur ce critère que les clients sélectionnent les équipementiers. Ils doivent en effet toujours veiller à ce que le recours à ces technologies

INTERVIEW

Michel Van Den Berghe
CEO Orange Cyberdéfense

ne soit pas un facteur de fragilisation de leur organisation. Il en est de même pour la 5G, qui va permettre de développer de nouveaux usages en lien avec les fonctionnalités de cette technologie.

Le phénomène des fake news est apparu ces dernières années. Orange intervient-il pour gérer ces infox ?

Nous n'avons pas vocation à intervenir sur les sujets de société. Mais, nous participons activement à la protection de l'information de nos clients. A ce titre, Orange Cyberdéfense effectue une veille 24h/24 sur les réseaux sociaux, les forums du Dark Net, les magasins d'applications et les plateformes de gestion de noms de domaine.

Le but ? S'assurer que les données de nos clients (marques, identités des dirigeants, noms de produits, informations stratégiques...) ne sont pas publiées indûment ou dénigrées abusivement sur ces réseaux. Nous protégeons ainsi leur actif informationnel en permettant, si besoin, le retrait d'informations frauduleuses, comme par exemple des noms de domaine usurpés.

Quels sont les grands enjeux autour de la cybersécurité en Afrique ?

Il est évidemment difficile de généraliser sur les enjeux globaux à l'échelle d'un continent aussi diversifié que l'Afrique. Toutefois, j'observe que la transformation numérique joue un rôle majeur dans la création de valeur et de ce fait, elle doit être accompagnée par la confiance numérique. C'est-à-dire la prise de conscience des problématiques cyber. Cela implique que les innovations intègrent la sécurité by design, la sensibilisation des utilisateurs, la formation des développeurs aux bonnes pratiques, la réalisation de tests réguliers de sécurité, ainsi que la capacité à détecter les incidents de sécurité, mais aussi leur anticipation.

Le renforcement de la réglementation est un autre enjeu important. Elle impose en effet aux entreprises et aux institutions de monter en maturité sur les sujets de sécurité numérique. Et fixe également les règles relatives aux traitements des données sensibles et notamment les données personnelles.

Par ailleurs beaucoup d'entreprises sont panafricaines et vivent donc au quotidien la nécessaire conformité avec différentes législations. La coopération des Etats en matière de cybersécurité est donc primordiale dans l'interception des pirates, qui sévissent eux-mêmes depuis plusieurs pays.

Enfin, tout cela ne sera rendu possible que par le développement du capital humain, via le financement de programmes cyber dans les parcours académiques. Et par le développement d'un écosystème regroupant universitaires, entreprises, Etats, recherche, Start-up, etc.

L'Afrique est-elle plus exposée que le reste du monde aux cyber-risques ?

Bien que les nations développent leurs stratégies de cybersécurité, leurs moyens humains, financiers et technologiques, ainsi que leurs dispositifs réglementaires ne sont pas encore aux niveaux attendus. Ainsi, la mise en application des mesures n'est parfois pas alignée à la menace des pirates sur leur territoire. Ils redoublent d'ingéniosité et sont peu dissuadés par l'arsenal législatif, au regard des gains potentiels.

D'autre part, les Etats africains ayant particulièrement investis dans les infrastructures télécoms dans les années 2000, cela se traduit par un taux de pénétration du mobile

autour de 100% sur l'Afrique francophone (https://developer.orange.com/orange_explains/marche-mobile-afrique-francophone/). Cela a permis le saut technologique que le continent connait et l'émergence de nouveaux services numériques (Mobile Payment, Mobile Money, digitalisation des parcours clients, etc.), via les synergies entre les banques et les opérateurs télécoms.

Ce bond technologique implique, de ce fait, une dépendance forte à ces services numériques qui ont révolutionné les usages du quotidien et se sont inscrits dans les mœurs.

Un des exemples le plus marquants étant le lancement d'Orange Money, déployé pour la première fois en Côte d'Ivoire, en 2008, et avec plus de 45 millions de clients en 2019, dans 18 pays. Orange Money compte un volume d'un milliard d'euros de transactions par semaine (https://www.orange.com/fr/Groupe/Activites/Services-financiers/Folder/Orange-Money). La paralysie de ce type de service peut donc entrainer un risque systémique.

De plus, l'utilisation massive de logiciels contrefaits rend le continent africain particulièrement vulnérable aux attaques cyber.

Dans un rapport de 2018, l'association BSA (Business Software Alliance) estime en effet que 80% des logiciels en Afrique (82% pour l'Algérie, 79% pour la Côte d'Ivoire, 64% pour le Maroc, 74% pour le Sénégal, 73% pour la Tunisie) sont piratés ou contrefaits, ce qui rend impossible leurs mises à jour et le support éventuels d'éditeurs.

En conclusion, le manque de moyens humains et financiers, tout comme la difficulté de mise en œuvre de la réglementation, couplée à l'exposition induite par le « jump » technologique et l'utilisation massive de logiciels contrefaits, tout cela expose très fortement le continent africain aux risques cyber.

Orange est un acteur important dans la finance digitale en Afrique. Compte tenu de la sensibilité de ce domaine, comment sécuriser les transactions et garantir la confiance ?

La confiance numérique est effectivement un élément essentiel pour le Mobile Banking et dans son utilisation à large échelle.

La sécurisation des transactions et des solutions mises à disposition des utilisateurs est donc primordiale. Cette sécurisation nécessaire implique la mise en œuvre d'une combinaison de plusieurs dispositifs notamment :

- La sécurité by design
- Réaliser des revues de code applicatif durant le processus de développement d'applications : il s'agit de vérifier que le code ne contient pas de faille de sécurité ;
- Former les développeurs d'applications transactionnelles aux bonnes pratiques de sécurité ;
- Mettre en place des solutions d'authentification forte (multi facteur ou intelligent) pour s'assurer de la bonne identification et autorisation du client.
- Auditer régulièrement les applications utilisées par les clients à travers des tests d'intrusion visant à identifier les vulnérabilités éventuelles.
- Mettre en place des campagnes de sensibilisation destinées aux clients, notamment concernant les e-mails frauduleux qu'ils pourraient recevoir au nom de la banque.
- Mettre en place des dispositifs de détection et se préparer à réagir en cas d'incident, afin de limiter l'impact et la persistance d'une attaque cyber.

Michel Van Den Berghe est Directeur général d'Orange Cyberdéfense depuis le 1er juillet 2014. Il a rejoint le groupe en janvier 2014, suite au rachat d'Atheos, dont il était le Président Fondateur depuis 2002.

Il est également le fondateur des Rencontres de l'identité, de l'audit et du management de la sécurité (RIAMS), qui réunissent depuis dix ans les principaux responsables et donneurs d'ordre du domaine de la sécurité des Systèmes d'Information.

Orange Cyberdéfense rassemble toute l'expertise en Cybersécurité d'Orange Business Services et compte 1 200 collaborateurs dans 220 pays.

« La menace cyber matérialise la guerre économique dans laquelle nous sommes entrés »

Alors que le potentiel de création économique par le secteur digital n'a jamais été aussi important, notamment sur le continent africain, les menaces cyber deviennent aussi de plus en plus fortes. Comment alors protéger les entreprises, les Etats et les citoyens des menaces de cybersécurité ? Francis Meston, Directeur Afrique, Moyen Orient d'Atos, l'un des leaders internationaux de la transformation digitale, répond à nos questions.

Francis Meston
Directeur Atos Afrique, Moyen Orient

CIO Mag : Quels sont les grands enjeux de la cybersécurité, notamment en Afrique ?

Francis Meston : La menace cyber matérialise la guerre économique dans laquelle nous sommes entrés. Elle se mesure aujourd'hui à travers l'augmentation et la montée en intensité des cyberattaques visant les entreprises et les organismes publics, voire les citoyens.

Les enjeux sont nombreux. Ils concernent la sensibilisation/éducation du grand public aux risques cyber (le facteur humain est à l'origine de la plupart des cyber-attaques), la formation et le recrutement d'ingénieurs cyber, ainsi que l'identification de nouveaux risques. En effet, les menaces évoluent rapidement avec l'arrivée de nouvelles attaques de plus en plus sophistiquées.

Pour l'Afrique, les enjeux sont peut-être encore plus élevés, puisque le continent tire parti de la révolution digitale dans tous les domaines et les industries. Parmi eux, la santé, les services financiers, l'agriculture, l' e-government.

La part de l'économie numérique constitue 25% du PIB au niveau mondial, soit l'équivalent de 20 000 milliards de dollars par an. En Afrique, l'économie numérique représente 7%.

Proportionnellement au PIB, le potentiel de création de richesse économique par le numérique est donc encore plus élevé en Afrique et les enjeux s'en trouvent décuplés.

Cette création de richesse et d'amélioration de la vie des citoyens sera possible seulement si le citoyen n'a aucun doute sur la sécurité des transactions,

Francis Meston
Directeur Atos
Afrique, Moyen Orient

INTERVIEW

sur la protection des données et sur la protection de sa vie privée. Assurer la confiance est l'enjeu fondamental de la cyber-sécurité.

L'Afrique est-elle plus exposée que le reste du monde en termes de menaces sur la cybersécurité ? Pourquoi ?

Comme le reste du monde, l'Afrique est exposée et les menaces y sont tout aussi fortes. Cependant, le continent a une spécificité : son développement numérique est basé sur le téléphone mobile (avec une forte utilisation du paiement mobile par exemple).

La protection des services de connectivité est donc clé, plus encore qu'ailleurs. Par exemple, plus de 500 millions de personnes utilisent le paiement mobile en Afrique centrale et de l'ouest, bien plus que dans n'importe quel autre continent dans le monde.

Les opérateurs de télécoms comme Orange Money, Safari Com ou les banques, tels Société Générale Yup, pour ne citer que quelques exemples, ont réussi à gagner la confiance de leurs clients en leur assurant toute la sécurité nécessaire. Il est primordial de continuer dans cette voix pour favoriser l'inclusion financière et plus généralement, l'inclusion citoyenne avec la sécurité nécessaire.

En quoi l'introduction de nouvelles technologies (5G, IOT) favorise-t-elle une expansion des cyberattaques ? Comment faire face ?

L'introduction de ces nouvelles technologies augmente les surfaces d'attaques. Les moindres objets connectés constituent de potentiels risques s'ils ne sont pas correctement sécurisés. En 2025, le nombre d'objets connectés au niveau mondial dépassera 20 milliards, selon de nombreux experts.

En 2030, on estime que la majorité des données sera stockée hors du Cloud ou des data centers et au plus prés des objets connectés (Edge Computing). Ce sont autant de points d'entrée dans les systèmes qu'il faut protéger. La 5G va faciliter et accélérer le développement de l'IoT et des Smart-Cities.

Les attaques vont désormais viser des villes, des entreprises et des citoyens de plus en plus connectés. La cybersécurité est donc essentielle pour protéger les villes et les Etats face à une expansion exponentielle des points d'entrée et des vulnérabilités.

Pour y faire face, il faut identifier et référencer tous les équipements et points d'entrée, les protéger et analyser en permanence les événements relatifs à la sécurité de ces équipements.

Ceci afin de repérer les attaques, qui de toute façon ne manqueront pas d'arriver, d'en limiter leur impact et de réagir en termes de minutes et non de semaines ou de mois, comme c'est encore le cas dans une majorité d'entreprises ou d'organisations.

Quel rôle doivent jouer les entreprises privées pour accompagner les Etats à renforcer la cybersécurité et la protection des données des citoyens ?

Aujourd'hui, nous assistons à une véritable prise de conscience du potentiel de développement économique lié à la digitalisation.

L'émergence d'une stratégie numérique à visée citoyenne et économique est en marche dans la majorité des états du monde.

Il s'agit de la digitalisation de l'identité (permettant l'inclusion citoyenne de tous), de la digitalisation des services

financiers (permettant l'inclusion financière), de la digitalisation des processus de soin (permettant l'inclusion sanitaire), de la digitalisation de l'agriculture (contribuant à l'autonomie alimentaire) et plus généralement de la digitalisation de l'ensemble des industries.

La cybersécurité, c'est un métier. C'est une course permanente contre les cybercriminels. Le rôle des entreprises technologiques spécialisées en cyber sécurité, c'est de gagner cette course chaque jour pour protéger les avancées de la digitalisation et ainsi soutenir la croissance et l'inclusion par la digitalisation.

Au-delà, c'est aussi le moyen de garantir une certaine autonomie et de protéger la souveraineté des états.

Les entreprises ont également un rôle dans la sensibilisation du grand public et le développement local des compétences en cyber sécurité.

Comment Atos se positionne-t-il sur cette question de la cybersécurité ? Quelles sont les solutions proposées, notamment pour les entreprises ?

N°1 européen et parmi les leaders mondiaux de la cybersécurité, Atos dispose, en plus d'une équipe globale, de plus de 5 000 spécialistes, d'un réseau mondial de centres d'opérations de sécurité (SOC) et de 6 centres de Recherches et Développement composés de 700 ingénieurs en R&D.

Ces ingénieurs produisent plus de 100 brevets par an, qui viennent s'additionner au 1 200 déjà existants.

En particulier, Atos dispose d'un Centre de compétence cyber sécurité au Maroc et d'un SOC (Security Operating Center) au Sénégal. Ces centres sont capables d'apporter le meilleur des compétences et du savoir-faire Atos à ses clients en Afrique.

Atos propose, de bout en bout, des services et des solutions de cybersécurité. Nous intégrons les meilleures technologies de sécurité et offrons un portefeuille complet de solutions de sécurité, aidant ainsi nos clients à transformer le risque en valeur commerciale.

Dans le monde numérique, les clients ont besoin d'une stratégie de sécurité transparente, qui évolue en permanence en fonction des opportunités et des menaces numériques. Du conseil et de l'analyse initiale, à la mise en œuvre et à la gestion continue, Atos accompagne ses clients à chaque étape.

« la cybersécurité est l'une des principales priorités de Huawei »

Adnane Ben Halima
Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei Northern Africa.

CIO Mag : Huawei Technologies, en partenariat avec le gouvernement chinois, China Unicom et China Telecom, a soumis, à l'Union Internationale des Télécommunications, un projet de «New IP», lequel est également connu sous le nom de New Internet. Quels en sont les objectifs ?

Adnane Ben Halima : La nouvelle technologie d'Internet Protocol (New IP technology) est conçue pour l'avenir. La vision et la philosophie techniques qu'elle représente sont issues des recherches du groupe de réflexion « ITU-T Focus Group Technologies for Network 2030 (FG NET-2030) ».

New IP vise à fournir de nouvelles solutions technologiques IP, qui peuvent répondre à ces exigences et aux applications futures, comme l'Internet of Everything, les communications holographiques et la télémédecine. Les réseaux IP du futur doivent prendre en charge les réseaux IP de haute précision et déterministes (HPDN) et l'interconnectivité hétérogène de nombreux réseaux. Le New IP est l'une des approches proposées.

Quelle est la stratégie de Huawei pour sécuriser les réseaux de données de ses clients, notamment en Afrique ?

L'une des principales stratégies de développement de Huawei est l'élaboration et la mise en œuvre complète d'un système mondial d'assurance de la cybersécurité.

L'entreprise s'est basée sur la conformité de toutes les lois et de toutes les réglementations nationales et régionales applicables en matière de sécurité, et sur les normes internationales de télécommunications. Huawei a ainsi établi un système d›assurance de la sécurité durable et fiable en termes de politiques, d›organisations, de processus, de gestion et de technologies.

Le Groupe travaille avec les gouvernements, les clients et les partenaires industriels pour relever les défis de la sécurité de manière ouverte et transparente. Et pour répondre pleinement aux exigences des clients en matière de cybersécurité. Huawei promet également de placer la responsabilité de l'entreprise avant ses intérêts commerciaux.

Afin de garantir que les ingénieurs fournissent uniquement des logiciels corrects aux clients, Huawei a spécifié le processus d›installation lors de la sortie, du téléchargement et de la livraison des logiciels. Pour tout opérateur, nous effectuons une vérification des antécédents, de la publicité, de la formation et des signatures d'engagement afin d'améliorer la gestion de la sécurité du personnel.

INTERVIEW

Adnane Ben Halima

Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei Northern Africa.

Aujourd'hui, Huawei fournit des infrastructures de télécommunications dans presque tous les pays africains et au siège de l'Union européenne (UE). Comment évaluez-vous le niveau de maturité et de sécurité des données qui y transitent ?

Pour le Groupe CFI basé aux États-Unis, les résultats de l'enquête menée pendant trois années consécutives, auprès de 177 opérateurs et de 12 300 personnes interrogées dans le monde entier, indiquent que la satisfaction des clients, ainsi que la fiabilité et la stabilité des équipements Huawei, sont bien supérieures à la moyenne du secteur.

Depuis 2013, Huawei a commencé à coopérer avec Cigital (basé également aux États-Unis) sur l'évaluation BSIMM de la sécurité, de la conception, de l'ingénierie et de la gestion des tests des équipements de Huawei.

Cette coopération s'est effectuée sur une base annuelle, couvrant 12 pratiques de sécurité (gouvernance de la sécurité, conception, codage, tests de sécurité, etc.).

Huawei a obtenu des résultats positifs, supérieurs à la moyenne de l'industrie, dans les 12 pratiques de sécurité. Et s'est classé premier dans 9 pratiques de sécurité.

Les transporteurs sont responsables de l'exploitation courante du réseau. Huawei n'a pas accès au réseau et à ses données.

Lorsqu'une défaillance se produit sur le réseau d'un opérateur, le Groupe fournit l'assistance technique et les services de dépannage nécessaires, et accède au réseau minimum et aux données du réseau de l'opérateur avec l'autorisation du client.

Dans un avenir proche, nous allons entreprendre le déploiement de réseaux 5G et la généralisation des objets connectés. Comment pouvons-nous garantir des déploiements plus sûrs pour les États ?

L'objectif de la sécurité du déploiement du réseau 5G est de garantir la sécurité des données des utilisateurs, des données du réseau, des actifs du réseau, des applications de service, etc.

Les dispositifs de réseau 5G doivent être conformes aux normes de sécurité NESAS & SCAS définies par la GSMA et le 3GPP, et doivent effectuer la configuration et le durcissement de la sécurité.

Deuxièmement, nous assurons la sécurité des données. Pour empêcher le vol ou l'altération des données, nous déterminons qui peut y accéder pendant le déploiement. Il faut crypter les données pendant le stockage et la transmission, effacer les données en toute sécurité après utilisation, et vérifier, par le biais du backtracking, qui a accédé aux données et à quel moment.

Troisièmement, afin de garantir la sécurité des biens et des services, un mécanisme de défense approfondi doit être mis en place pendant le déploiement du réseau. Ceci dans le but de s'assurer, grâce à un balayage de sécurité périodique, que le réseau ne présente pas de vulnérabilités et de risques potentiels.

L'UE a approuvé le déploiement de réseaux 5G en Europe avec des infrastructures fournies par Huawei. Comment appréciez-vous cet engagement européen ?

Huawei se félicite de la décision de l'Europe, qui lui permet de continuer à participer au déploiement de la 5G sur le continent. Nous continuerons à travailler

avec les gouvernements et l'industrie européens pour développer des normes communes, afin de renforcer la sécurité et la fiabilité du réseau.

Les gouvernements des États membres de l'UE devraient soutenir une plus grande collaboration entre les secteurs public et privé. Cela favoriserait l'acceptation et la mise en œuvre généralisées des normes internationales de comportement responsable, et des mesures de confiance dans le cyberespace.

Face aux accusations portées contre Huawei de recueillir des données auprès de ses utilisateurs par le biais d'écoutes, certains fabricants d'équipements ont assuré qu'ils comprenaient l'attitude de votre groupe, car cette pratique est courante dans cette industrie. Partagez-vous cette analyse ?

La cybersécurité et la protection de la vie privée des utilisateurs sont les principales priorités de Huawei. Huawei n'a jamais eu et n'aura jamais accès secrètement aux réseaux de télécommunications et nous n'en avons pas la capacité. Huawei n'est qu'un fournisseur d'équipements.

À ce titre, il serait impossible d›accéder aux réseaux des clients sans leur autorisation et sans qu›ils ne s'en aperçoivent.

Nous n'avons pas la capacité de contourner les opérateurs et le contrôle d'accès, et n'avons pas davantage la possibilité de prendre des données sur leurs réseaux sans être détectés par tous les pare-feux ou par les systèmes de sécurité normaux.

Qu'est-ce qui vous différencie des autres fournisseurs d'équipements ?

Tout d'abord, nos services sont orientés vers les clients pour maintenir des opérations de réseau stables, fiables et sécurisées dans toutes les situations, telles que les catastrophes naturelles, les conflits ou les piratages.

La cybersécurité et la protection de la vie privée sont nos principales priorités. Au cours des trente dernières années, Huawei a servi plus de 3 milliards de personnes dans le monde entier, en soutenant le fonctionnement stable de plus de 1 500 réseaux d'opérateurs dans plus de 170 pays et régions.

Nous avons également investi plus de 10 % de notre chiffre d'affaires annuel dans la R&D, soit 131,7 milliards de CNY (18,9 milliards de $US) en 2019, ce qui représente 15,3 % du revenu total de la société.

Enfin, le Groupe compte 15 000 employés engagés dans la recherche, dont plus de 700 docteurs spécialisés en mathématiques, plus de 200 docteurs spécialisés en physique et en chimie, et plus de 5 000 docteurs spécialisés en ingénierie.

Adnane Ben Halima a été nommé au poste de Vice-Président en charge des relations publiques pour la région Méditerranée de Huawei, le 6 mai 2020.

A 40 ans, il est titulaire d'un diplôme d'ingénieur en informatique. Il a débuté sa carrière professionnelle en tant qu'ingénieur en recherche et développement chez ST-Microelectronics, avant de rejoindre Huawei Technologies, en 2005.

Adnane Ben Halima a également piloté le lancement de plusieurs nouveaux réseaux 3G, 4G, THD fixe et plateforme Cloud dans plusieurs pays du continent, ainsi que le lancement de nouveaux opérateurs télécoms.

MAROC
Le digital, levier de l'accélération de l'enseignement supérieur

La transformation digitale, si elle n'est pas une fin en soi, peut constituer un nouveau paradigme dans la création de valeur par et pour les établissements d'enseignement supérieur. Plus globalement, il est aujourd'hui de notoriété publique que le développement de l'usage des TIC est une condition essentielle de l'égalité des chances, de la compétitivité de la croissance économique et de l'emploi.

La maîtrise de l'outil informatique par les étudiants, mais aussi par leurs encadrants, constitue désormais un socle de compétences que nul ne peut ignorer. Nous ne nous attarderons donc pas sur l'impérieuse nécessité de la maîtrise d'un tel outil, aujourd'hui devenue une nécessité, mais aussi un élément de différenciation, mais plutôt sur les enjeux qui sous-tendent le déploiement de l'usage du numérique dans l'enseignement supérieur. Ils sont essentiellement de trois natures :

Pédagogique, en utilisant de manière performante les nouvelles possibilités des TIC dans l'enseignement. Des MOOC[1] aux Serious Games, en passant par la réalité virtuelle, les possibilités sont multiples.

Elles permettent dans un premier temps de répondre à la problématique de la massification et du sous-encadrement, et dans un second temps de proposer de nouvelles techniques d'apprentissage pédagogique, centrées sur l'acquisition de compétences. Quelques initiatives ont néanmoins le mérite d'exister, notamment celles de :

- l'EMI, qui a mis en place un campus numérique offrant un service de formation à distance et une bibliothèque numérique ;
- L'université Hassan II, qui a déployé une plateforme MOOC ;
- L'initiative Maroc Université Numérique.

Cela implique évidemment que les étudiants et leurs encadrants puissent être équipés en matériel adéquat. A ce titre, il convient de souligner l'existence du programme INJAZ, qui, chaque année, s'appuie sur une offre de services des opérateurs de télécommunications constituée d'un pack étudiant comprenant un service Internet haut débit et un ordinateur portable léger[2].

Maroc Université Numérique

La plateforme Maroc Université Numérique, dédiée à des cours en ligne ouverts et massifs, a été officiellement lancée au Maroc le 12 juillet 2019 à Rabat. Développée en partenariat entre le ministère de l'Education nationale et le groupement français d'intérêt public "GIP FUN-MOOC", cette plateforme, première en son genre au Maroc et en Afrique, vise aussi à développer des cours en ligne privés à des petits groupes (SPOC) et à promouvoir la coopération entre les universités marocaines et françaises en matière de formation à distance commune, adaptée aux spécificités de l'enseignement supérieur au Maroc.

La plateforme propose des contenus dans des domaines variés : l'éducation et la formation, les sciences de l'ingénieur, l'informatique, l'économie et les finances, les sciences fondamentales, la santé, les langues, le management et l'entreprenariat, l'environnement, les sciences humaines et le droit.

La plateforme, dont l'accord de création a été signé en juillet 2016, vise à fédérer les projets des universités et écoles marocaines pour leur donner une visibilité internationale.

1 Massive Open Online Course : type ouvert de formation numérique à distance capable d'accueillir un grand nombre de participants. L'appellation MOOC est passée dans le langage courant en France ; elle est désormais reconnue par les principaux dictionnaires

2 Sont bénéficiaires, une seule fois, tous les étudiants (élèves ingénieurs et assimilés) inscrits en vue de l'obtention d'un diplôme national dans les établissements d'enseignement supérieur public partenaires de l'initiative «10.000 Ingénieurs», à savoir : Ecoles d'ingénieurs, Facultés des Sciences et Facultés des Sciences & Techniques

- Institutionnelle, en offrant aux décideurs les outils leur permettant de maîtriser en temps réel l'actualité des établissements et de piloter leur performance.

  La mise en œuvre d'un système d'information cohérent, articulé et harmonisé constitue sans aucun doute un véritable catalyseur dans la remontée d'indicateurs, à toutes les mailles décisionnelles, permettant de suivre les développements « sur le terrain », de prendre les décisions;

- Sociale et sociétale, en fournissant aux élèves et aux enseignants des services innovants pour améliorer la vie étudiante, mais aussi en leur donnant les moyens de comprendre les enjeux de société, les enjeux économiques et stratégiques liés à ces technologies.

De plus, si certains établissements disposent des moyens d'acquérir des ERP universitaires, d'autres se retrouvent dans l'obligation de « faire avec les moyens du bord », afin de proposer aux étudiants des applications leur permettant de consulter les archives de cours en ligne par exemple.

L'aspect financier est donc déterminant pour permettre à ces établissements d'entamer leur transformation digitale.

La transformation digitale de l'enseignement supérieur marocain nécessitera donc, dans le cadre d'un schéma directeur national du numérique, cohérent et rationnel, de développer de manière concomitante :

- Les infrastructures et équipements : mettre à disposition de la communauté éducative l'infrastructure et les services adaptés aux usages ;

- Les services numériques : généraliser l'accès et l'usage d'espaces numériques de travail et d'administration pour les étudiants et le personnel encadrant ;

- Les usages et ressources numériques : en complément des services numériques, le développement des usages nécessite d'être accompagné par une politique de production, de diffusion et de mutualisation des ressources pédagogiques ;

- La formation au numérique et l'accompagnement : la généralisation de la maîtrise des outils digitaux dans les pratiques pédagogiques implique de fortes actions de formation et d'accompagnement de l'ensemble de la communauté éducative.

Le code informatique, nouvel ascenseur social ?

Et si le digital, et plus particulièrement la programmation informatique, devenait le nouvel ascenseur social du Maroc, notamment en réponse aux taux de déperditions scolaire et à l'insertion sur le marché de l'emploi ?

L'économiste en chef de la Caisse des Dépôts et de Gestion affirme que la polarisation de la société marocaine, qui va bien au-delà du concept d'inégalités, est essentiellement sous-tendue par l'ampleur du chômage des jeunes, qui trouve lui-même son origine dans la maîtrise insuffisante de la langue française, en particulier chez les jeunes diplômés.

Son hypothèse se base, entre autres, sur le constat selon lequel le français (ou l'anglais d'ailleurs, ndlr) est la langue d'acquisition des compétences techniques, scientifiques et professionnelles, mais d'abord et surtout celle des employeurs.

L'économiste affirme également que la maîtrise du français est particulièrement faible au sein de la jeunesse marocaine et se trouve fortement déterminée par l'origine sociale.

A ce titre, les chiffres du dernier rapport du Programme National d'Evaluation des acquis Scolaires (PNEA) sont accablants : les élèves des écoles publiques maîtrisent seulement 23% du programme de français, contre 37% pour les élèves des écoles privées.

Le Maroc tente de réformer son secteur éducatif depuis plusieurs années, mais il peine toujours à se relever d'une léthargie pluri décennale, ponctuée par des plans d'urgence dont les effets restent limités.

En 2019 encore, les remous politiques provoqués par la loi-cadre sur l'éducation relèvent d'un anachronisme qui prend tout sens dès lors que l'on observe, même de loin, le produit des systèmes éducatifs étrangers, dont l'excellence se mesure, entre autres, à l'aune

des progrès technologiques qui nous envahissent chaque jour : des voitures autonomes à l'expérience client hyper personnalisée, en passant par les thérapies biotechnologiques ; le « numérique » se trouve partout, tout le temps, avec pour substantifique moelle des milliers de ligne de code et d'algorithmes.

A titre d'exemple, l'intelligence artificielle, ou le machine learning, qui est aujourd'hui sur toutes les langues, est une compilation informatique d'algorithmes capables d'auto-apprentissage, c'est-à-dire en mesure de progresser « intellectuellement » et de manière autonome dans l'exercice de la fonction qui leur est assignée.

Les Américains ont très vite compris qu'il était encore plus pragmatique d'apprendre aux enfants à programmer le numérique, au-delà de simplement l'utiliser.

En 2013, Barack Obama a lancé la semaine de l'informatique à l'école, au cours de laquelle tous les jeunes américains devaient créer leur propre jeu vidéo.

En 2014, le Royaume-Uni a donné le top départ d'un programme d'initiation pour les enfants à partir de l'âge de 5 ans.

Une question simple se pose alors : pourquoi ne pas faire du code un langage d'enseignement universel au Maroc, sans bien sûr occulter les autres disciplines scolaires telles que les sciences humaines, l'art et la culture, et plus généralement ce que l'on appelle les soft skills ? Il ne s'agit pas là de remettre en question la pédagogie des langues, mais plutôt d'introduire une nouvelle discipline en mesure de faire éclore des compétences jusque-là inexploitées. Pour ce faire, il conviendrait :

- D'introduire la programmation informatique comme véritable langue vivante et d'intégrer dans le cursus pédagogique des jeunes élèves dès les premières classes;
- De mettre en place des programmes de formation courts, à une maille régionale, en mesure d'inculquer les fondamentaux du code et capables d'offrir une réelle compétence aux apprentis. Des programmes comme le « Wagon », une formation intensive au développement Web de 9 semaines qui apprend à coder entièrement des applications Web, en sont une belle illustration ;
- De généraliser l'apprentissage du code dans l'enseignement supérieur, notamment via un modèle pédagogique dédié, s'appuyant sur des cycles de formation courts, professionnalisants et « agiles ». Par « agile », nous entendons une adaptation permanente aux exigences du marché de l'emploi marocain.

Face à une jeunesse marocaine à 2 vitesses, dont une grande partie est sacrifiée sur l'autel des langues étrangères, la généralisation et la maîtrise de la programmation informatique permettrait à terme de :

- Disposer d'une nouvelle génération de capital humain, spécialisée et formée rapidement, disposant des qualifications nécessaires pour accompagner la transformation digitale de la société marocaine ;
- Renforcer l'équité dans l'insertion professionnelle, face aux nouvelles exigences du marché de l'emploi, permettant, à terme, de réduire la dichotomie sociétale qui accentue cette polarisation socio-économique du Maroc ;
- Promouvoir la fibre entrepreneuriale de jeunes apprentis possédant désormais les armes pour mettre à exécution leurs idées, constituant par effet d'entraînement un véritable levier de création d'emplois ;
- Pallier le départ massif de ces compétences tant prisées par les employeurs étrangers, et transformer cette tendance en avantage pour le Maroc : produire des ambassadeurs au lieu d'envoyer des immigrés ;
- Capter les nouvelles compétences africaines, dans la mesure où le continent a pris le virage digital de façon plus avancée dans certains pays (Kenya, Rwanda, Ghana, etc.), et faire ainsi du Maroc un véritable hub des emplois et compétences africains.

Ainsi, à l'heure où l'on parle

de leapfrog digital africain[3], ou « d'accélération industrielle digitale » au Maroc[4], l'apprentissage généralisé du « code » semble être une fantastique opportunité pour réaliser le bond en avant tant espéré.

Deux recommandations, sur le digital au Maroc, pourraient être suivie :

- **Développer les budgets associés à l'investissement digital.**

Le déploiement de tels moyens nécessitera indéniablement la conception d'un schéma directeur numérique national pour l'enseignement supérieur, cohérent, rationnel, et préconisant le développement de manière concomitante des infrastructures et équipements ;

- **Instaurer le code informatique comme une langue vivante à part entière et en faire un véritable levier « d'accélération académique »**.

Son apprentissage nécessite peu de prérequis, et offre une seconde chance, notamment pour les lauréats déclassés, de réintégrer le circuit professionnel à travers des formations professionnalisantes, agiles et de courte durée (6 mois en moyenne).

Former une nouvelle génération de capital humain orientée « digital » permettra non seulement de pallier les départs massifs de cette ressource rare, mais aussi de donner les moyens techniques et technologiques aux futurs entrepreneurs de mettre leurs idées à exécution, tout en répondant à une demande pressante du tissu économique pour cette catégorie de capital humain.

3 Huet, Jean-Michel, Africa and the digital leaprog, Pearson, 170 pages, 2018

4 Déclaration de Moulay Hafid El Alami, Ministre de l'Industrie, de l'Investissement, du Commerce et de l'Economie Numérique, au salon Vivatech 2019

Jean-Michel Huet, Associé, Afrique et développement International, **Saleh Cherquaoui**, Senior Manager, Bureau de Casablanca, **Soukaina Kadiri** & **Marie Heipp**, consultantes, Bureau de Casablanca.

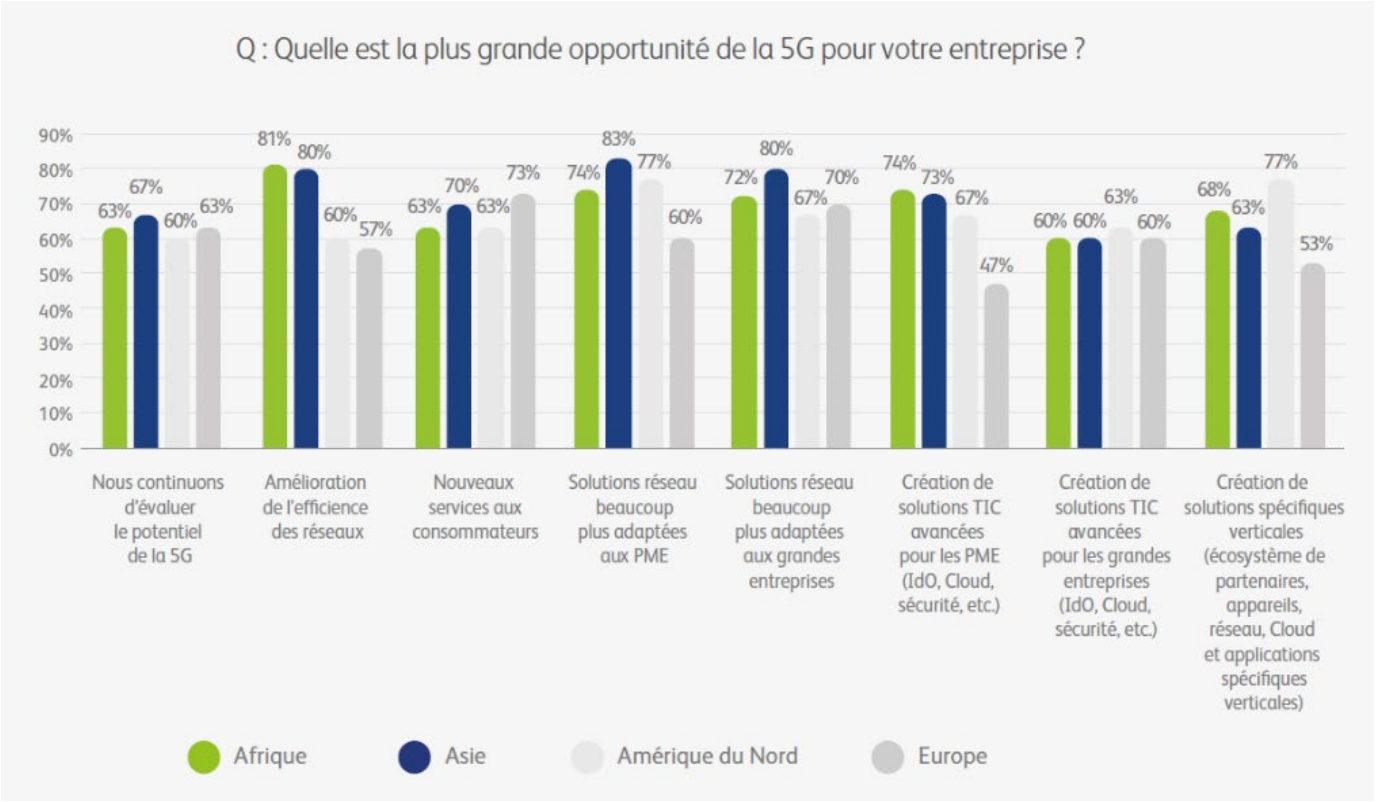
BEARING POINT

La 5G, un enjeu B2B en Afrique

2020 : une nouvelle décennie et le véritable début de l'ère de la 5G. Au début de l'année, 33 opérateurs télécoms, à travers 18 pays, ont lancé des services commerciaux 5G et 77 prévoyaient également de le faire en 2020. Alors qu'ils doublent désormais leurs investissements dans la 5G, les opérateurs télécoms doivent agir concrètement pour voir un retour sur investissement.

Jean-Michel Huet, associé Bearing Point

La 5G est différente. En ce qui concerne la monétisation, la GSMA prévoit que la 5G sera la première génération de technologies mobiles à avoir un impact plus important sur les entreprises que sur les consommateurs. Les observateurs du secteur sont d'accord. Plus important encore, de nombreux opérateurs télécoms le sont également. Mais si le B2B est l'« étoile polaire »[1] des revenus de la 5G, personne ne semble avoir établi une feuille de route indiquant aux opérateurs comment l'atteindre. En effet, il y a plus de questions que de réponses concernant l'opportunité B2B de la 5G. Quels sont les cas d'utilisation gagnants ? Quel segment (PME ou grandes entreprises) représente la plus grande opportunité ? Quelle est l'importance des offres génériques horizontales par rapport aux services verticaux spécialisés ? Les entreprises achèteront-elles auprès des opérateurs télécoms ou feront-elle appel à d'autres fournisseurs ? Quel est le rôle des opérateurs télécoms dans la chaîne de valeur de la 5G ?



En Afrique, l'arrivée de la 5G sera plus tardive que dans d'autres régions, mais l'impact sur le B2B est bien perçu, notamment par certains acteurs pour qui le B to B est le nouvel « eldorado » des télécoms en Afrique. Il est vrai que le segment a été un peu négligé au profit des offres prépayées B2C. L'impact semble particulièrement capital pour les PME, avec la spécificité que cette gamme d'entreprises représente l'essentiel du tissu économique. Certains domaines, notamment autour de l'Internet des objets (IoT) ou

les innovations au croisement des sujets télécoms et utilities (électricité notamment), sont aussi des sujets d'intérêt. Source : BearingPoint, 2020

En Afrique, plus que dans les autres régions du monde, bâtir un écosystème autour des services que pourraient apporter la 5G fait sens. Les opérateurs télécoms ont un vrai rôle à jouer dans ce domaine, car ils sont naturellement les orchestrateurs de ces écosystèmes. Dans les domaines économiques où la 5G peut apporter un vrai « saut quantique », la capacité des opérateurs à animer ces écosystèmes est fondamentale.

Certains secteurs paraissent être au cœur de cette transformation : les transports (notamment les zones portuaires), le développement de zones urbaines connectées, les usages du digital dans l'agriculture, la connectivité pour changer la donne dans l'énergie, le domaine de la santé et enfin celui de l'éducation. En s'inscrivant dans une logique d'écosystème, la dynamique est alors double.

Bien sûr, les entreprises travaillant dans ces domaines - notamment les PME africaines - seront au cœur de cette transformation et seront donc des clients directs des opérateurs télécoms.

Mais, et c'est le deuxième effet, ces PME et quelques grands groupes pourront aussi être des partenaires pour bâtir de nouveaux modèles économiques hybrides en visant d'autres clients entreprises ou clients grand public.

Dans ce modèle, les liens avec les Etats et les financements des bailleurs de fonds sont aussi une dimension à intégrer.

Cette étude nous aide à comprendre ce que les opérateurs télécoms doivent devenir et comment ils doivent se positionner pour évoluer vers « l'étoile polaire » des revenus B2B de la 5G.

Les grandes entreprises et les PME estiment que la 5G sera importante pour leurs activités. Elles pensent que les opérateurs télécoms ont beaucoup à leur offrir en termes de produits et services 5G - certainement plus que les simples offres de connectivité et d'infrastructure informatique de l'ère de la 4G - et elles envisageraient sans réserve d'acheter chez eux.

La destination étant claire et la voie tracée, la vraie question est la suivante : y a-t-il une réticence des dirigeants à s'éloigner de leur domaine traditionnel pour œuvrer dans les domaines adjacents de l'orchestration des cas d'usage ? Le changement de modèle économique est-il trop risqué pour les dirigeants qui ont construit leur carrière en améliorant leurs réseaux ?

L'enjeu est-il de gérer les attentes des actionnaires institutionnels, lesquels souhaitent que les opérateurs télécoms maintiennent des dividendes élevés et n'augmentent pas les investissements dans de nouveaux domaines ? Ou s'agit-il d'une incapacité perçue à effectuer des changements - attirer de nouveaux talents, mettre en place de nouvelles méthodes de travail et aborder la gestion des produits et des écosystèmes de manière plus agile et expérimentale - dans de grandes organisations ?

Ce qui est clair, cependant, c'est que les opérateurs télécoms n'ont pas une minute à perdre. Les entreprises n'attendent pas la 5G et n'attendent certainement pas les opérateurs télécoms. Elles agissent maintenant, s'associent et collaborent avec des fournisseurs qui peuvent les aider à résoudre leurs problèmes.

La 5G nécessite un modèle économique fondamentalement différent de celui de la 3G et de la 4G pour générer un retour sur investissement. Les opérateurs télécoms doivent élever leur réflexion sur leur propre position sur le marché. Ils doivent voir la situation dans son ensemble.

Ils doivent choisir un marché vertical et s'y lancer. Ils doivent collaborer avec ces clients. Ils doivent co-innover et co-créer avec un large éventail de fournisseurs traditionnels, de cyber-entreprises, d'acteurs technologiques, de spécialistes de marchés verticaux et même de concurrents.

Jean-Michel Huet, associé BearingPoint

1 Voir l'étude de BearingPoint, « Le B2B, l'étoile polaire des revenus de la 5G », 32 pages, mai 2020, étude auprès de plus de 300 entreprises en Europe, Asie, Amérique et Afrique.

Le Covid-19, la confiance numérique et l'Afrique

Ibrahima Nour Eddine DIAGNE
Président d'African Performance Institute

La crise du Covid-19 et les logiques de sortie du confinement ont conduit plusieurs gouvernements à accorder une importance de premier rang aux technologies de l'information. Le débat le plus féroce actuellement porte sur les limites de l'usage (volontaire ou involontaire) des technologies de tracking pour maitriser la pandémie. En effet, le tracking (traçage numérique) est considéré comme une entrave lourde aux libertés et en même temps, il semble être le levier le plus solide pour contrer l'expansion incontrôlée de la pandémie.

Sur un autre registre, l'usage intensif des outils de télé-conférence et de télé-travail ne s'entoure plus des précautions habituelles sur la protection des données (vidéo, message, texte). Personne ne se préoccupe de la sécurisation des conversations à travers des outils cloud. Chacun accepte l'outil que lui propose son interlocuteur.

Nous sommes sans doute entrés dans une nouvelle ère de redéfinition de la notion de liberté, de sécurité et de confiance. Il se passe sans doute des choses inimaginables en matière de violation des règles et des principes, aussi bien par les Etats, les entreprises que les gros opérateurs numériques. Le citoyen se retrouve ainsi piégé dans cette tourmente, laquelle ne laisse à présent la place qu'aux seules revendications conférant plus de quiétude et garantissant une reprise économique.

Comment l'Afrique vit-elle ces chamboulements ?

Du fait que l'espace numérique n'est pas la réplique exacte de celui dans lequel les Nations exercent traditionnellement leur souveraineté, aucun pays ne peut en réalité prétendre appliquer sa souveraineté dans son espace numérique.

Les pays africains, comme tous les autres, ont des lois et se donnent les moyens de les faire appliquer. Cependant, il faut reconnaître que pour ce qui est de l'espace numérique, notre contrôle est souvent limité en raison du déficit de moyens technologiques.

Et notre souveraineté est parfois écorchée par des réglementations venant de l'étranger.

Elles s'imposent naturellement à nos entreprises et à nos citoyens simplement parce qu'il n'y a aucune alternative nationale.

La maîtrise de l'espace numérique est de moins en moins l'affaire des Etats et de plus en plus l'affaire des «giga» entreprises du numérique. L'Afrique n'en disposant pas, elle est particulièrement vulnérable.

Dans ce contexte de crise du Covid-19, la souveraineté numérique est à mon sens une fiction, qui ne doit pas mobiliser les débats et les énergies. Il faut plutôt se concentrer sur la maîtrise de l'espace numérique, laquelle passe nécessairement par une convergence entre les intérêts des gouvernements, du secteur privé et des citoyens du continent. Il faut une stratégie cohérente, de sorte que les plateformes qui collectent les données sanitaires et de géolocalisation des citoyens soient le plus possible soumises aux lois du pays et conformes aux valeurs et au modèle de société.

Le Covid-19 est venu bousculer l'ordre des urgences. Le chantier est vaste et les aspects juridiques et technologiques sont de loin les leviers les moins cruciaux. La priorité, c'est qu'une véritable révolution mentale se produise et que la culture africaine soit placée au cœur des préférences des populations. Les choix politiques, ceux des entreprises et des citoyens doivent nourrir un écosystème numérique qui ne soit plus extraverti. Il faut des ponts de confiance entre les gouvernements et le secteur privé africain.

Le monde va se refermer pour un petit moment avec cette crise du Covid-19. A charge pour les Africains de compter sur eux-mêmes, a l'instar de ce que fera chaque région du globe.

Nous ne pouvons plus continuer à sponsoriser la dissémination des données de nos populations vers qui veut. Nous devons commencer à bâtir des stratégies pour apporter ou susciter des alternatives.

La question de l'endroit où se trouvent les serveurs est une distraction, si on la compare à la propension de n'importe quel acteur à collecter des données sensibles des populations d'un pays. Avoir des réponses africaines à ces questions est plus valable que de se barricader dans nos frontières à coup de lois, sans avoir la force de faire valoir nos préoccupations.

La construction de la zone continentale de libre échange continental est une occasion pour construire un dispositif stratégique cohérent. Il peut favoriser la création de valeur endogène pour soutenir les économies africaines et les protéger.

Ces enjeux sont prioritaires car tout retard accusé se rattraperait difficilement. Les réglementations ont pour vocation de protéger des industries ou de favoriser leur éclosion.

L'Afrique doit être très vigilante car l'ère post Covid-19 décidera des gagnants et des perdants.

CORONAVIRUS
Des mesures d'hygiène pour réduire les risques de cyberattaques

A l'heure de la mise en place des mesures de confinement liées à la crise sanitaire du Covid-19, bon nombre de DSI ont eu des sueurs froides pour satisfaire aux exigences de la continuité d'activité dans plusieurs secteurs.

Arnaud Fléchard
CTO de Kleverware

En effet, partout où cela a été possible, il a fallu, dans un laps de temps très court, mettre en place un recours massif au télé-travail pour les collaborateurs tout en n'ayant pas systématiquement l'intégralité des ressources pour le faire dans les meilleures conditions. Car mettre en place le télé-travail de manière pertinente signifie bien souvent, donner accès à un plus grand nombre de collaborateurs qu'à l'accoutumé au cœur du Système d'Information de l'entreprise avec les risques et des brèches potentielles de sécurité que cela suppose. Cela est d'autant plus vrai quand les cyber-pirates saisissent l'opportunité pour multiplier les tentatives de hacking et que dans le même temps, les collaborateurs chargés de prémunir l'entreprise de ces attaques, sont eux-mêmes partiellement indisponibles.

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a émis en des temps plus calmes un *« Guide d'Hygiène Informatique »* pour redonner de la perspective aux bonnes pratiques en la matière. Certaines de ces recommandations résonnent avec d'autant plus de force en ce moment. Rappelons-en quelques-unes qui semblent clé.

Au premier chef, l'expansion de l'accès à distance au SI de l'entreprise, via la mise en place du télé-travail, implique d'avoir un nombre croissant d'utilisateurs des services de mobilité informatique, qui ne sont pas nécessairement au fait des bonnes pratiques en matière de sécurité. Il est bon de rappeler qu'une part notable des attaques informatiques « réussies » impliquent d'une manière ou d'une autre l'humain et donc principalement les collaborateurs de l'entreprise victime, bien souvent « sans penser à mal » ou par « inadvertance » mais au mépris de certaines règles de base. Il est donc primordial de former et d'informer notamment les nouveaux utilisateurs nomades pour limiter la vulnérabilité du SI.

Ensuite, aussi bien du côté des administrateurs du réseau informatique de l'entreprise que des responsables des lignes Métier, il convient d'avoir une vision claire des accès autorisés au(x) système(s) de l'entreprise : tout le monde n'a probablement pas besoin d'avoir accès à l'intégralité des applications ou des données de l'entreprise. La revue des comptes à privilèges et la revue des droits d'accès doit être régulière afin de s'assurer que les accès aux éléments sensibles soient maitrisés.

Disposer de procédures d'autorisation et d'authentification doit permettre de circonscrire les problèmes, de faciliter la surveillance et de détecter plus facilement les éventuelles brèches ou attaques.

Enfin, mettre en place quelques garde-fous parait indispensable pour sécuriser l'information propriété de l'entreprise, l'un des risques majeurs étant la fuite de celle-ci. Cette lutte se joue sur plusieurs tableaux : il s'agit dans le même temps de limiter les possibilités de « sortir » des informations (bannir les supports amovibles, limiter l'envoi d'e-mails vers des comptes externes...) mais aussi de sécuriser les connexions avec le réseau de l'entreprise via la mise en place de VPN respectant les dernières normes de sécurité.

Cette crise ayant eu un effet dynamisant sur la mise en place du télé-travail, celui-ci est probablement amené à s'inscrire dans la durée au sein des organisations où cela est possible. Il n'est donc jamais trop tard pour se préparer à mettre en place des fondations saines pour que le risque ne l'emporte pas sur l'opportunité.

Vers la souveraineté numérique de l'Afrique

Le cyber-colonialisme est un sujet très controversé. D'aucuns disent qu'en parler dans un langage moins provocateur serait bénéfique à la réflexion tandis que d'autres soulignent qu'un débat contradictoire sur la question doit effectivement avoir lieu. Quoiqu'il en soit ... que signifie le cyber-colonialisme pour l'Afrique et que pouvons-nous concrètement faire pour engager le continent sur le chemin de la cyber-indépendance ?

Youssef Travaly
Vice-président
du Next Einstein Forum

A l'aube de la Quatrième Révolution Industrielle (4RI), le pouvoir transformateur des technologies numériques se fait de plus en plus ressentir, modifiant notre mode de fonctionnement et d'interaction au sein de nos sociétés. Le rôle central que le numérique à joué en ces temps de pandémie en est la preuve. Il est par ailleurs évident que les effets que cette digitalisation accélérée de l'économie formelle et informelle que nous vivons va perdurer au-delà de la pandémie nous amenant déjà à repenser notre modèle de société.

La quatrième révolution se caractérise notamment par l'usage concomitant de sources énergétiques durables et de technologies numériques, toutes deux transversales à divers secteurs économiques. Cette transversalité de la 4RI la rend ainsi indispensable à la croissance économique de l'Afrique. En témoigne, à titre d'illustration, l'économie basée sur les moyens de paiement « mobile » qui a contribué à hauteur de 8,6% au PIB de l'Afrique (144 milliards de dollars américains) en 2018 et 14 milliards de dollars de recettes fiscales en 2017. Ces paiements « mobile » ont par ailleurs joué un rôle central et déterminant dans les mesures de distanciation sociale et les mesures barrières en matière de prévention du COVID-19.

Dans le domaine de l'agriculture, la technologie numérique offre des opportunités considérables pour améliorer le bien-être des populations en jouant un rôle central dans le développement durable du secteur. La santé est un autre domaine à fort potentiel de transformation numérique.

En effet, la majorité des pays africains se caractérisent par des systèmes de santé sous-financés et inadéquats, situation difficile encore accentuée par des lacunes infrastructurelles considérables. Les chaînes d'approvisionnement et les secteurs de la logistique sont également les grands bénéficiaires du digital, surtout en matière de pistage de cargaisons, de facilitation du commerce inter-États et d'inclusion sociale.

La prolifération des technologies numériques a également donné naissance à de nouvelles économies telles que la « gig economy », synonyme de grandes sociétés américaines comme Uber et Airbnb dont l'impact s'est étendue à divers autres pays du monde.

Bras de fer entre les États-Unis et la Chine

Cependant, nombre de risques sont associés au déploiement massif des nouvelles technologies en particulier celui de la cyber-colonisation du continent. En effet, les technologies digitales, telles que l'Intelligence artificielle qui sous-tendent la 4RI, s'appuient sur des algorithmes basés sur les données, celles-ci parfois biaisées car fonction de l'échantillonnage de population utilisé pour leurs développements. Il est par conséquent primordial d'analyser cette numérisation

rapide des économies africaines, sous l'angle de son processus, des valeurs et des motivations sous-jacentes. A défaut, cela peut mener à l'avènement du cyber-colonialisme, déjà fortement contesté par nombre d'individus et d'organisations dans les pays développés.

Il est évident que la course à l'IA est fortement dominée par les États-Unis et la Chine. En Afrique, les États-Unis dominent au niveau de l'architecture de l'écosystème numérique tandis que la Chine est en tête sur le plan des infrastructures au travers de la fourniture de téléphones mobiles bon marché via des sociétés chinoises telles que Huawei et ZTE.

Par ailleurs, la plupart des technologies d'IA sont développées sur des marchés plus riches en raison des coûts prohibitifs et des compétences spécialisées requises pour les construire, même là où elles sont destinées à être utilisées dans les pays en développement.

Le discours géopolitique de la cyber-colonisation semble donc être principalement axé sur le bras de fer entre les États-Unis et la Chine, et ce au détriment des consommateurs, notamment africains, laissés-pour-compte lors de la conception des produits. Néanmoins, malgré ces risques d'exploitation pour l'Afrique, l'IA a un rôle important à jouer dans la transformation technologique et donc économique de l'Afrique.

Les pays africains sont donc à la croisée de chemins critiques où les décisions et les investissements détermineront aujourd'hui si l'Afrique devient cyber-colonisée ou s'ils peuvent prétendre à l'exploitation de l'IA pour accélérer leurs développements. Quelles sont nos recommandations ?

Souveraineté numérique

Si l'Afrique veut atténuer les effets de la cyber-colonisation, des investissements substantiels doivent être faits pour assurer la décentralisation d'Internet et plaider pour des logiciels libres et ouverts créés par des Africains. En outre, comme le souligne à juste titre le sociologue Michael Kwet, *« si l'Afrique veut atteindre à une quelconque forme d'indépendance numérique, nous devons plutôt enseigner à nos enfants comment «Google», l'Internet fonctionne, ce qui se cache derrière, plutôt que de se limiter à l'utilisation pure et simple de ses produits. »*

Les principaux domaines de contestation en Afrique sont l'extraction des données personnelles, l'ensemble de l'architecture numérique, les populations non connectées et plus largement les lois commerciales internationales qui favorisent les États occidentaux et la Chine. Les menaces de cyber-colonisation existent aux niveaux étatique, sociétal et individuel et comprennent des menaces à la souveraineté des nations, aux libertés individuelles et à la vie privée.

Sur le plan réglementaire, les États doivent être proactifs en élaborant une législation qui protège les droits fondamentaux de leurs citoyens tout en promouvant l'innovation, la recherche et le développement. L'accès sans entraves aux populations et aux discours politiques (principalement via les plateformes de médias sociaux) ouvre la porte à une ingérence politique pour des gains géopolitiques par des parties externes grâce à un profilage psychologique rendu possible par le Big Data et l'IA. Le scandale de Cambridge Analytica et l'utilisation de l'Afrique comme terrain d'essai pour l'ingérence politique sont une indication de la vulnérabilité des pays en développement, sans les infrastructures et les connaissances nécessaires pour bloquer de telles intrusions.

Cette souveraineté numérique ne peut être atteinte qu'en reconnaissant le caractère interdisciplinaire des technologies de l'IA et en proposant des interventions sur le front socio-économique, politique et technologique.

Une infrastructure de base et spécifique à l'économie est une condition préalable, ancrée sur un environnement politique et réglementaire solide, établissant de nouvelles formes de partenariats et fournissant un financement adéquat pour la recherche et le développement et chacune de ces interventions pour être mise en œuvre avec succès. Le développement du capital humain est une intervention clé pour habiliter les jeunes esprits africains à construire des solutions qui servent leurs communautés et les marchés mondiaux – faites par eux pour eux.

Les ressources économiques et démographiques de l'Afrique la placent finalement à l'épicentre des futures cyber-guerres entre les superpuissances numériques du monde. Le continent n'est pas impuissant. Grâce à des efforts stratégiques et concertés, au renforcement des capacités à travers les infrastructures, les politiques et les compétences, en empruntant aux meilleures pratiques d'autres marchés émergents, l'Afrique peut être un moteur de l'IA.

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

CALENDRIER ÉDITORIAL 2020

N°62 Janvier-Février

Haut débit (broadband) et croissance d'Internet (mobile) en Afrique
Bilan, Enquêtes et perspectives

N°63 Mars – Avril

Focus sur l'identité numérique en Afrique, l'autre enjeu de souveraineté

N°64 Mai - Juin

Spécial Sommet Afrique France 2020, ville durable

N°65 Juillet – Août

Cybersécurité, protection des données personnelles, confiance numérique:
l'Afrique est-elle plus exposée que le reste du monde?

N°66 Septembre - Octobre

Fintech, eCommerce et écosystème de la finance digitale en Afrique

N°67 Novembre – Décembre

L'humain au cœur de la transformation
Dossier pays: Le Maroc

DOSSIERS ABORDÉS EN 2019

LA RÉFÉRENCE DU NUMÉRIQUE EN AFRIQUE

Oui, je souhaite m'abonner

Afrique subsaharienne

❑ 1 an	47 500 FCFA /73 €
❑ 2 ans	95 000FCFA /145 €
❑ 3 ans	142 500 FCFA /217 €

Europe et Maghreb

❑ 1 an	42 500 FCFA /65 €
❑ 2 ans	85 000FCFA /130 €
❑ 3 ans	127 500 FCFA /195 €

Dom-Tom et reste du monde

❑ 1 an	50 000 FCFA /77 €
❑ 2 ans	100 000 FCFA /154 €
❑ 3 ans	150 500 FCFA /231 €

*Frais de port inclus dans le prix

Nom ..... **Prénom** .....

Société ..... **Fonction** .....

Adresse de livraison .....

Boîte postale .....

Code postal ..... **Ville** ..... **Pays** .....

Tél. ..... **Fax** .....

E-mail .....

Je règle la somme de ..... €

❑ Chèque de banque à l'ordre de SAFREM Sarl

❑ Transfert bancaire (BNP Paribas Paris.

IBAN : FR76 3000 4029 3300 0100 3689 160 - BIC : BNPAFRPPPCE

Bulletin d'Abonnement à retourner à :

SAFREM Sarl - 23 Rue Colbert 78180

Saint-Quentin en Yvelines France

Tél : +33 1 30 64 80 24 / cio@cio-mag.com

http://www.cio-mag.com/sabonner

Date et signature

L'exploration
nous éclaire sur la voie à suivre

La recherche constante de l'innovation est un gage d'éclairage pour le monde intelligent

HUAWEI

Nos solutions de cybersécurité pour garantir votre souveraineté numérique

Trusted partner for your **Digital Journey**

Atos