adf
AFRICA DEFENSE FORUM

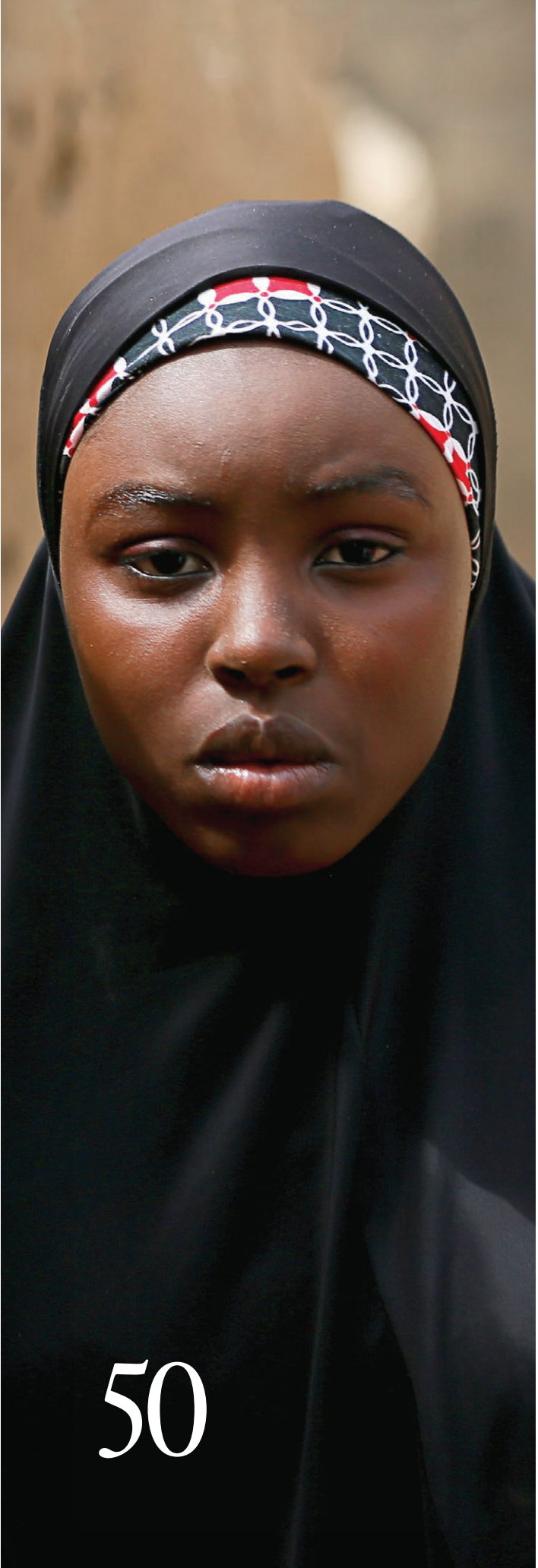
UN WEB DE MENACES, UN UNIVERS DE PROMESSES

Alors que l'Afrique comble l'écart du numérique, elle doit améliorer sa cybersécurité

VISITEZ-NOUS EN LIGNE : ADF-MAGAZINE.COM

TABLE DES MATIÈRES

articles



50

rubriques

EN COUVERTURE : Cette illustration représente les connexions numériques du monde et souligne le besoin d'une cybersécurité améliorée pour défendre la croissance économique de l'Afrique. ILLUSTRATION D'*ADF*

POINT DE VUE

À une certaine époque, un commandant militaire pouvait déclarer confortablement : « Je ne suis pas informaticien », ou « Je n'utilise pas vraiment l'Internet ».

Cette attitude n'est plus une option.

Être un professionnel de la sécurité aujourd'hui, cela veut dire faire face aux menaces qui se cachent dans le cyberespace. Les adversaires étrangers peuvent attaquer les systèmes d'armement, mettre la vie des soldats en danger et créer le chaos sur les réseaux des chemins de fer, de la distribution d'eau et de l'électricité.

Connaître les questions cybernétiques, ce n'est pas seulement connaître les menaces. Cela veut dire être confortable pour utiliser les ordinateurs afin d'accéder aux informations et de communiquer. La technologie ne soutient pas seulement la mission de défense moderne, elle est au cœur de cette mission.

Les professionnels de la sécurité essaient partout de mieux travailler. Cela commence par la formation dans les universités nationales et les collèges d'état-major, et cela se poursuit avec une formation en milieu de carrière. Les forces armées doivent faire de la cybersécurité une spécialité distinctive et assurer que tous les soldats aient un niveau minimum de compétence informatique.

Le moment est aussi venu d'examiner le rôle des forces armées dans la protection contre les attaques cybernétiques. Des pays tels que l'Afrique du Sud et le Nigeria créent des commandements cybernétiques et d'autres nations développent des spécialités cybernétiques au sein des structures de commandement existantes. Cela devrait coïncider avec un dialogue national concernant le rôle que les forces armées peuvent et devraient jouer dans la cybersécurité.

Enfin, les professionnels de la sécurité doivent pratiquer la sensibilisation cybernétique. Les menaces évoluent et les meilleures pratiques de l'hygiène cybernétique doivent aussi évoluer. Toute personne qui ne sait pas comment identifier des attaques par hameçonnage ou éviter un maliciel ou un logiciel de rançon met en danger un réseau complet. Les protocoles de sécurité multi-niveaux et l'identification des menaces internes sont tout aussi importants.

L'accès à l'Internet augmente plus rapidement en Afrique que partout ailleurs dans le monde. Le continent et ses économies comptent désormais sur l'Internet de haut débit. Les professionnels de la sécurité doivent être prêts à jouer leur rôle pour assurer que le cyberespace reste sécurisé.

Personnel de l'état-major unifié des États-Unis pour l'Afrique

Des soldats vérifient l'équipement de communication pendant Africa Endeavor, exercice de communication militaire annuel organisé par l'état-major unifié des États-Unis pour l'Afrique.

ÉTAT-MAJOR UNIFIÉ DES ÉTATS-UNIS POUR L'AFRIQUE

adf AFRICA DEFENSE FORUM

Cyber-sécurité

Volume 12, 2ème trimestre

L'ÉTAT MAJOR UNIFIÉ DES ÉTATS UNIS POUR L'AFRIQUE

POUR NOUS CONTACTER

U.S. AFRICA COMMAND
Attn: J3/Africa Defense Forum
Unit 29951
APO-AE 09751 U.S.A.
ADF.EDITOR@ADF-Magazine.com

HEADQUARTERS
U.S. AFRICA COMMAND
ATTN: J3/AFRICA DEFENSE FORUM
GEB 3315, ZIMMER 53
PLIENINGER STRASSE 289
70567 STUTTGART
GERMANY

ADF est un magazine militaire professionnel trimestriel publié par l'état-major unifié des États-Unis pour l'Afrique qui permet au personnel militaire africain de bénéficier d'un cadre international propice aux échanges. Les opinions exprimées dans ce magazine ne reflètent pas nécessairement les principes ou points de vue de cette organisation ni d'aucune autre agence du gouvernement des États-Unis. Certains articles sont écrits par l'équipe d'*ADF*, tout autre contenu est noté avec la source d'origine. Le Secrétaire à la Défense a déterminé que la publication de ce magazine est nécessaire à la conduite des affaires publiques, conformément aux obligations légales du Département de la Défense.

La sécurisation du cyberespace de l'Afrique

Cheikh Bedda, directeur du département de l'infrastructure et de l'énergie de la Commission de l'Union africaine, *s'est exprimé devant l'atelier sur les cyberstratégies, la cyberlégislation et la création des CERT (équipes de réponse aux urgences informatiques) pour tous les états membres de l'UA le 23 juillet 2018 à Addis-Abeba (Éthiopie). Ses remarques ont été modifiées pour les adapter à ce format.*

Comme le reste du monde, l'Afrique accueille à bras ouverts son avenir numérique. Les leaders africains se sont engagés à développer l'économie numérique et la numérisation des secteurs stratégiques tels que l'éducation, la santé, l'entreprenariat, l'emploi, la paix et la sécurité, et la bonne gouvernance en facilitant la fourniture des services publics et en multipliant les interactions entre le gouvernement et le peuple.

Sur le continent, il existe de nombreuses histoires numériques à succès qui doivent être dupliquées dans les autres pays pour promouvoir la croissance économique et le développement social. Toutefois, plus notre économie est numérisée et connectée, plus il devient important de sécuriser nos systèmes dans le cyberespace.

Aujourd'hui, les pays africains affrontent tout un éventail de menaces cybernétiques, de cybercrimes, d'attaques, d'activités d'espionnage et autres activités malveillantes. En général, ils n'ont pas les moyens de surveiller et de contrôler leurs réseaux, ce qui les expose à des risques qui peuvent affecter leur sécurité nationale et leur économie.

À mesure que les pays africains améliorent leur accès à la connectivité large bande, ils deviennent plus interconnectés et vulnérables aux attaques cybernétiques. Il devient crucial de renforcer nos aptitudes humaines et institutionnelles pour sécuriser le cyberespace en développant une foi et une confiance dans l'utilisation des cybertechnologies par les états et les habitants d'Afrique.

Selon le rapport « Les tendances de la cybersécurité et la cybercriminalité en Afrique » que nous avons publié en collaboration avec Symantec en 2016, de nombreux pays africains n'ont pas encore adopté les instruments de politique et les structures législatives nécessaires pour combattre l'utilisation malveillante de la technologie de l'information et des communications (TIC). Huit pays seulement possèdent des stratégies nationales de cybersécurité et treize pays africains seulement ont établi des équipes nationales de réponse aux urgences informatiques.

La sécurité et la stabilité de notre cyberespace africain commun s'appuient sur les capacités locales et nationales de coopération de tous les pays dans le but de prévenir les incidents cybernétiques et d'y réagir, et d'effectuer des enquêtes et des poursuites visant la cybercriminalité et le cyberterrorisme.

Du point de vue de la Commission de l'Union africaine (CUA), un cyberespace résilient et sécurisé dépend du succès de la mise en œuvre et de l'exécution d'une stratégie holistique de la cybersécurité, notamment le développement d'un écosystème riche avec de fortes structures législatives et un savoir-faire technique qui assure le contrôle pour sécuriser les réseaux et protéger l'infrastructure critique.

Des participants du Gabon (à gauche) et de la République du Congo prennent part à un exercice de cybersécurité lors d'Africa Endeavor 2018 au Cap-Vert.

ÉTAT-MAJOR UNIFIÉ DES ÉTATS-UNIS POUR L'AFRIQUE

Pour affronter les défis dus aux crimes commis par l'utilisation de la TIC, la 23ème assemblée des chefs d'état et de gouvernement de l'UA a adopté en 2014 la Convention sur la cybersécurité et la protection des données. Connue aussi sous le nom de Convention de Malabo, elle se concentre sur les règles de sécurité essentielles visant à créer un environnement numérique crédible et à permettre de développer une société moderne de l'information en Afrique.

Toutefois, quatre ans après son adoption, seulement trois pays – la Guinée, l'île Maurice et le Sénégal – ont fourni à la CUA des actes de ratification. Son entrée en vigueur nécessite 15 ratifications.

Nous devons protéger notre cyberespace africain commun en tant que bien partagé et aussi en tant que responsabilité partagée, pour assurer sa sécurité et son accessibilité par tous nos habitants.

Nous pensons qu'une cybersécurité forte est une composante clé de la transformation numérique de l'Afrique. Aussi est-il important d'améliorer nos capacités en développant des politiques et une législation cybernétiques et en accroissant la sensibilisation à tous les niveaux sur les avantages et les menaces liés à l'utilisation des services numériques.

AFP/GETTY IMAGES

LA RÉCOLTE DES SAUTERELLES, TRÈS APPRÉCIÉES EN OUGANDA, EST EN BAISSE

BBC NEWS À BBC.CO.UK/NEWS

Pendant la saison des sauterelles en Ouganda, ces insectes bouillis ou frits sont considérés comme un mets fin et nutritif. Ils sont si populaires que certains se préoccupent de la baisse de la récolte.

« Lorsque la saison commence, nous observons le cycle de la lune et nous nous préparons. [Elles ont tendance à sortir pendant la pleine lune.] Nous espérons aussi qu'il pleuvra », déclare Quraish Katongole, l'un des trappeurs de sauterelles les plus expérimentés de l'Ouganda. « Elles sortent en plus grand nombre après la pluie. »

Ses employés placent des tonneaux dans un lieu de capture près de la ville de Masaka. À mesure que la nuit descend, ces insectes au corps mince grouillent autour des lampes. Les trappeurs brûlent de l'herbe fraîche et la fumée s'élève, ce qui étourdit les insectes. Les sauterelles percutent les tôles et tombent dans les barils.

Pendant les heures de pointe dans la capitale de Kampala, des jeunes gens se faufilent à travers le trafic pour vendre aux conducteurs des sauterelles bouillies ou frites et prêtes à manger. Une cuillère à soupe coûte 1.000 shillings ougandais (27 cents).

Les Ougandais sont parmi les 2 milliards de personnes dans le monde qui mangent des espèces différentes d'insectes. Un rapport de 2013 de l'Organisation des Nations unies pour l'alimentation et l'agriculture recommande fortement aux autres d'envisager de les ajouter à leur régime alimentaire, en déclarant que cela pourrait améliorer la nutrition et l'approvisionnement alimentaire.

Des vendeurs ambulants vendent de petites portions de sauterelles frites à Kampala (Ouganda).

Mais en Ouganda le nombre de sauterelles pourrait être en baisse à mesure que les habitats de nourriture et de reproduction reculent autour du lac Victoria.

Ceci est confirmé par le résultat du travail de la nuit. Les jeunes hommes vident les barils et ne peuvent remplir que deux sacs. « À un certain moment, je pouvais remplir 20 à 25 sacs par nuit », déclare M. Katongole.

Les chercheurs ougandais essaient de mieux comprendre le cycle de vie des sauterelles pour déterminer si elles peuvent être récoltées de façon plus durable. Le professeur Phillip Nyeko déclare que, en plus de la perte de leur habitat, les récoltes agressives constituent une autre menace.

« Elles ne grouillent pas pour être mangées ; elles grouillent pour se nourrir et pour se reproduire. Mais lorsque vous allumez des lampes et que vous en récoltez des milliers, vous perturbez leur cycle de vie », déclare le professeur Nyeko.

L'Afrique considère

LE BOOM DES JEUX MOBILES

AGENCE FRANCE-PRESSE

Une armée humaine dévaste une colonie d'extra-terrestres, alors que Simon Spreckley, créateur sud-africain de jeux vidéo, contrôle avec enthousiasme l'action à l'aide de l'écran tactile de son téléphone.

« La pénétration des appareils mobiles est énorme en Afrique. Les gens ont souvent deux ou trois téléphones, ce qui est assez dingue », déclare M. Spreckley, âgé de 40 ans. « C'est donc un grand avantage, et c'est la raison pour laquelle nous essayons de faire ça », déclare-t-il, en faisant la promotion d'*Invasion Day*, un jeu qui sera probablement lancé sur le magasin d'appli d'Apple et sur la plateforme Google Play en 2019.

Beaucoup d'autres développeurs africains choisissent aussi d'adapter des jeux pour les appareils mobiles au lieu des consoles traditionnelles ou des ordinateurs de bureau.

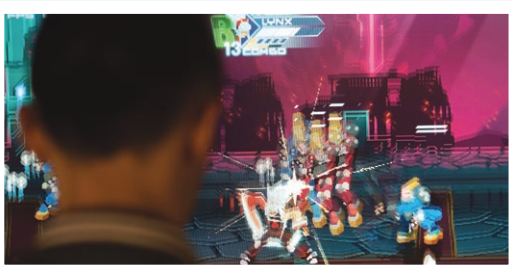
« Il existe un potentiel énorme en Afrique parce que le continent est principalement mobile », déclare Sidick Bakayoko, 34 ans, fondateur de Paradise Game, groupe de coordination pour les développeurs de Côte d'Ivoire. Il a rejoint les codeurs de jeu, les développeurs et les artistes africains qui se sont réunis avec les dirigeants de Sony et d'autres géants industriels lors de la convention de la Semaine des jeux africains au Cap.

M. Bakayoko déclare que le nombre croissant de produits ludiques africains pour les dispositifs portables reflète l'explosion des services bancaires et des outils financiers sur portable tels que Mpesa au Kenya.

M. Spreckley espère qu'*Invasion Day* suscitera l'intérêt d'un investisseur majeur, mais de nombreux développeurs africains de jeux mobiles ont eu des difficultés pour monétiser leurs créations. La décision de Google en juin 2018 permettant aux développeurs africains de jeux de gagner de l'argent en vendant leurs créations sur son magasin Google Play pourrait révolutionner le secteur.

« La plupart des gens utilisent Android [de Google] ici », déclare Sithe Ncube, 24 ans, fondateur de l'Ubongo Game Lab en Zambie. « Les gens n'avaient pas de moyen de monétiser leurs jeux mobiles. Cela fait bien quelques temps que les gens développent des applis, mais il n'y avait pas moyen de l'utiliser comme modèle commercial. »

Un délégué joue à un jeu de bagarre inédit appelé *Shattered Realms* [Royaumes anéantis] lors de la Semaine des jeux africains en novembre 2018 au Cap (Afrique du Sud). AFP/GETTY IMAGES



LES BANANES

AIDENT L'ANGOLA À RÉDUIRE SA DÉPENDANCE PÉTROLIÈRE

AGENCE FRANCE-PRESSE

Une employée nettoie, trie et emballe des bananes dans une ferme près de Caxito (Angola). AFP/GETTY IMAGES

Les boîtes de bananes vertes d'un empilement de cageots sont amenées l'une après l'autre dans un conteneur d'expédition réfrigéré à Caxito (Angola).

Les fruits, qui portent la marque « From Angola, with Love » [De l'Angola, avec amour], sont expédiés aux consommateurs à 6.000 kilomètres de distance. Cela s'inscrit dans le cadre des efforts entrepris par Luanda pour diversifier son économie et se libérer de sa dépendance pétrolière

Novagrolider, société privée, produit plusieurs douzaines de tonnes de bananes par semaine, qui sont expédiées au Portugal.

« Nous avons deux catégories : la production nationale et la production à l'exportation », déclare le superviseur Edwin Andres Luis Campos. « La production nationale sera vendue ici dans les supermarchés angolais dans quatre ou cinq jours environ. La production à l'exportation sera expédiée vers l'Europe dans des conteneurs réfrigérés qui arriveront dans 20 à 25 jours. »

La production de Novagrolider a augmenté exponentiellement au cours des dernières années et Grupolider, sa société-mère qui a aussi des intérêts dans les transports et l'immobilier, emploie 3.500 personnes.

Elle cultive des mangues, des ananas, des pastèques et des bananes dans ses quatre exploitations fruitières angolaises.

Après un démarrage prudent, l'ambition du chef d'entreprise João Macedo a grandi rapidement. M. Macedo espère doubler sa production à 170.000 tonnes par an et prendre pied en Afrique du Sud.

À Caxito, le premier responsable agricole de la province partage l'enthousiasme de M. Macedo.

« Nous fournissons des encouragements financiers aux petits agriculteurs pour qu'ils accroissent la superficie des zones qu'ils cultivent, déclare Eliseo Mateos. Jusqu'à présent, ils produisaient principalement pour leur subsistance, mais maintenant nous voulons qu'ils produisent plus pour qu'ils vendent leurs récoltes sur le marché. Les bananes sont notre "carburant vert" : nous avons ici une possibilité de diversifier l'économie. »

Au cours de la décennie qui a suivi une guerre civile sanglante de 27 ans, l'Angola a enregistré un fort taux de croissance de deux chiffres, alimenté par le pétrole qui est responsable pour 90 % des exportations de l'Angola et 70 % des revenus de l'état.

La baisse des prix du pétrole brut en 2014 a bouleversé le modèle économique du pays en provoquant une contraction. Si le pays augmentait sa production nationale, le besoin de devises étrangères pour acheter les aliments importés baisserait.

« Avec le soutien et l'organisation du gouvernement, le secteur agricole pourrait être la force motrice du développement de ce pays », déclare M. Macedo.

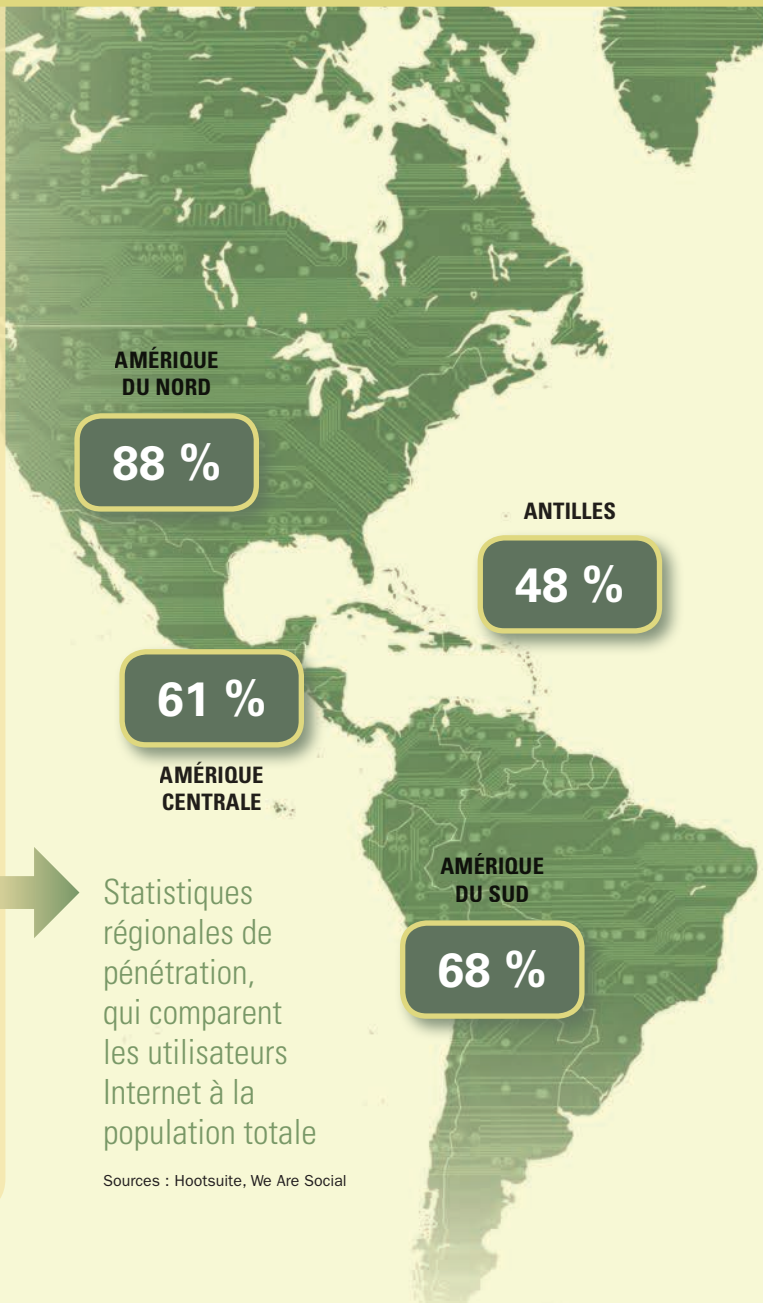
Un Web de MENACES, Un univers de PROMESSES

Alors que l'Afrique comble l'écart du numérique, elle doit améliorer sa cybersécurité

PERSONNEL D'*ADF*

La pénétration de l'Internet

La pénétration de l'Internet en Afrique accuse un retard par rapport à beaucoup d'autres régions du monde, mais le continent se rattrape rapidement. Les pays font de gros investissements en câbles à fibre optique et autre matériel pour rendre l'Internet accessible à toutes les classes économiques. **Entre 2017 et 2018, l'accès à l'Internet en Afrique a enregistré une croissance de 20 %,** le taux de croissance le plus rapide du monde. Au Bénin, au Mozambique, au Niger et en Sierra Leone, le nombre d'utilisateurs de l'Internet a plus que doublé pendant cette période. **Aujourd'hui, 52 pays africains sont connectés à des câbles Internet sous-marins ou à un réseau de fibre optique, et 44 % des habitants vivent à moins de 25 kilomètres d'un nœud de fibre optique** qui fournit un accès Internet à haut débit. Bien que cette croissance offre de nombreuses avenues pour le développement économique et l'amélioration de la gouvernance, elle s'accompagne de risques.



Statistiques régionales de pénétration, qui comparent les utilisateurs Internet à la population totale

Sources : Hootsuite, We Are Social

Les enfants d'une zone rurale du Bénin reçoivent une formation informatique.

AFP/GETTY IMAGES

EUROPE DU NORD
94 %

74 %
EUROPE DE L'EST

EUROPE DE L'OUEST
90 %

77 %
EUROPE DU SUD

50 %
ASIE CENTRALE

ASIE DE L'EST
57 %

MOYEN-ORIENT ET ASIE DE L'OUEST
65 %

ASIE DU SUD
36 %

49 %
AFRIQUE DU NORD

58 %
ASIE DU SUD-EST

39 %
AFRIQUE DE L'OUEST

AFRIQUE CENTRALE
12 %

27 %
AFRIQUE DE L'EST

69 %
OCÉANIE

51 %
AFRIQUE AUSTRALE

MOYENNE MONDIALE : 53 %

ILLUSTRATION D'*ADF*

LES ATTAQUES CYBERNÉTIQUES

Ce que disent les chiffres

Les attaques cybernétiques ont des conséquences financières. L'attaque par WannaCry a paralysé les banques, les hôpitaux et les agences d'état dans plusieurs pays, notamment au **Kenya** où les institutions financières ont été affectées. Au **Maroc**, une usine automobile Renault a été fermée pendant un jour, ce qui a arrêté la chaîne de production.

Dans l'ensemble du continent, le coût des attaques cybernétiques sur les économies s'élève annuellement à **3,5 milliards de dollars**. Ces crimes ont des degrés de gravité différents, depuis le vol des cartes de crédit qui provoquent des charges non autorisées, jusqu'au vol des secrets de la sécurité nationale qui met en péril la sécurité de millions de personnes.

En Afrique du Sud, l'un des pays les plus connectés du continent, **67 %** des adultes signalent qu'ils ont été victimes d'un cybercrime.

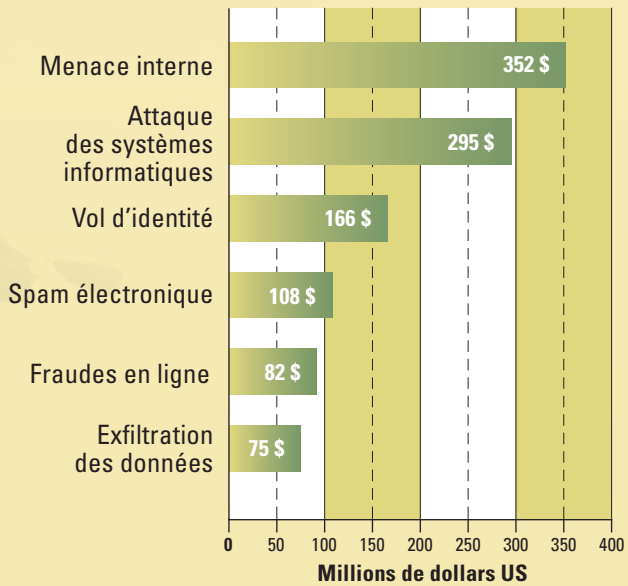
Perte annuelle moyenne pour chaque victime de la cybercriminalité : **274 dollars**

Source : Symantec

ILLUSTRATION D'ADF

Les types d'attaque les plus fréquents en Afrique et leurs coûts associés

Coût en 2017



Définitions

MENACE INTERNE
Un employé ou quelqu'un d'autre bénéficiant d'un accès privilégié utilise abusivement les données

ATTAQUE SUR LES SYSTÈMES INFORMATIQUES
Attaque externe conçue pour nuire à la fonctionnalité

VOL D'IDENTITÉ
Un hacker vole des données personnelles

SPAM ÉLECTRONIQUE
Messages conçus pour inciter l'utilisateur à divulguer des informations ou à cliquer sur un lien malveillant

FRAUDES EN LIGNE
Histoires fictives conçues pour inciter les utilisateurs à établir un rapport commercial ou personnel

EXFILTRATION DES DONNÉES
Suppression non autorisée des données

Source : Serianu

Les méthodes d'attaque

Les criminels s'adaptent constamment, en cherchant à exploiter de nouvelles vulnérabilités et en abandonnant les anciennes méthodes lorsqu'une défense a été développée. Bien que les attaques cybernétiques aient des milliers de formes, la plupart appartiennent aux catégories générales suivantes.

Logiciel de rançon

Ces attaques prennent le contrôle d'un ordinateur ou d'un réseau. En général, les pirates informatiques exigent le paiement d'une rançon pour libérer et/ou décrypter les données qu'ils ont saisies. Les attaquants obtiennent parfois accès à un ordinateur lorsque l'utilisateur clique sur un lien, mais dans d'autres cas ils sont capables d'infiltrer un réseau et de se déplacer automatiquement d'un ordinateur à un autre. Ces attaques deviennent de plus en plus fréquentes. Selon Help Net Security, il y a eu 181 millions d'attaques de logiciel de rançon au cours des six premiers mois de 2018, près du double des attaques pendant la même période de l'année précédente.

COMMENT L'ÉVITER

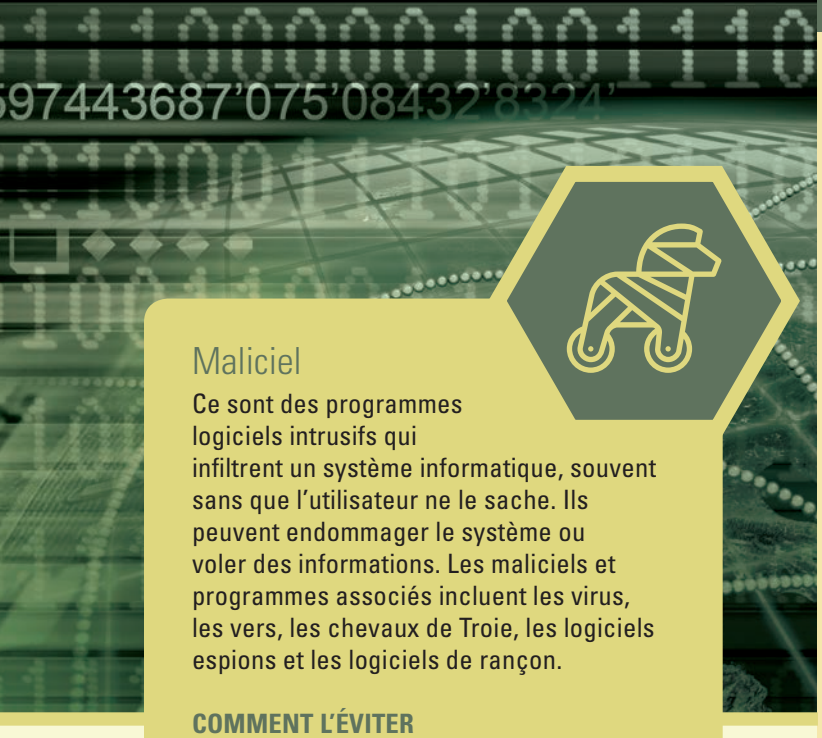
Utiliser un logiciel antivirus et un pare-feu lorsque cela est possible. Utiliser un réseau privé virtuel (VPN) pour accéder à l'Internet à partir d'une connexion Wi-Fi publique. Sauvegarder régulièrement tous les fichiers pour qu'ils puissent être récupérés en cas d'attaque. Finalement, en cas d'attaque par un logiciel de rançon, il ne faut pas payer la rançon. Cela ne fait qu'encourager les attaques futures et n'offre aucune garantie de récupération des données.

Fraudes par hameçonnage

Elles concernent en général un e-mail qui demande à l'utilisateur de cliquer sur un lien. Le lien pourrait conduire à un site qui imite un établissement financier ou un fournisseur d'e-mails. L'usager peut être amené à une page qui demande un nom d'utilisateur et un mot de passe sous prétexte que ce dernier doit être réinitialisé. L'intention véritable est de capturer le mot de passe de l'utilisateur pour que l'attaquant puisse accéder aux informations de la cible.

COMMENT LES ÉVITER

Ne pas cliquer sur les liens ou les fichiers joints ouverts provenant d'une source inconnue ou non fiable. Chercher des expressions suspectes dans les e-mails, par exemple des fautes d'orthographe, et chercher des adresses électroniques inhabituelles. Installer une barre d'outils anti-hameçonnage dans votre navigateur. La plupart des navigateurs Internet offrent des barres d'outils qui analysent les sites avant que l'utilisateur ne les visite pour déterminer si ce sont des sites de hameçonnage. Utiliser un pare-feu et un logiciel antivirus, et faire attention à tous les pop-ups. Ne jamais fournir d'information personnellement sensible ou financière à des sources inconnues ou non fiables. Les établissements respectables n'écrivent pas d'e-mail à leurs clients pour leur demander un mot de passe ou des informations personnelles. Il faut être méfiant.



Maliciel

Ce sont des programmes logiciels intrusifs qui infiltrent un système informatique, souvent sans que l'utilisateur ne le sache. Ils peuvent endommager le système ou voler des informations. Les maliciels et programmes associés incluent les virus, les vers, les chevaux de Troie, les logiciels espions et les logiciels de rançon.

COMMENT L'ÉVITER

Utiliser des pare-feu et des antivirus, ne pas visiter les sites non fiables ou télécharger le contenu de ces sites.

Attaque de point d'eau

Dans ce type d'attaque, les hackers observent ou devinent le site qu'une personne, un groupe ou des membres d'une organisation visiteront probablement. Les attaquants infectent ce site avec des maliciels ou autres virus nuisibles. Une fois que les cibles visitent le site, elles deviennent infectées, ce qui permet dans certains cas au maliciel de se propager vers d'autres membres de l'organisation. Les sites Internet réputés ne sont pas à l'abri de ces attaques. En 2013, des sites associés à Twitter, Facebook et Apple ont été compromis.

COMMENT L'ÉVITER

La dissimulation des mouvements en ligne à l'aide d'un VPN empêche les acteurs externes de pister certaines activités de navigation. En outre, la mise à jour des logiciels pour corriger les bogues et la surveillance des activités suspectes sur un réseau aident à empêcher les intrusions.

Cibles populaires

L'infrastructure critique, les industries, les banques et les systèmes d'armement sont numériquement connectés dans beaucoup de pays. Cela accélère le commerce mais rend les organisations vulnérables aux attaques cybernétiques. En 2017, une attaque appelée WannaCry s'est propagée globalement sur les systèmes informatiques. L'attaque a disséminé un code malveillant qui a paralysé certains systèmes et en a forcé d'autres à se mettre hors service de peur d'être attaqués.

Les secteurs africains les plus ciblés par les cybercriminels sont indiqués ci-dessous :

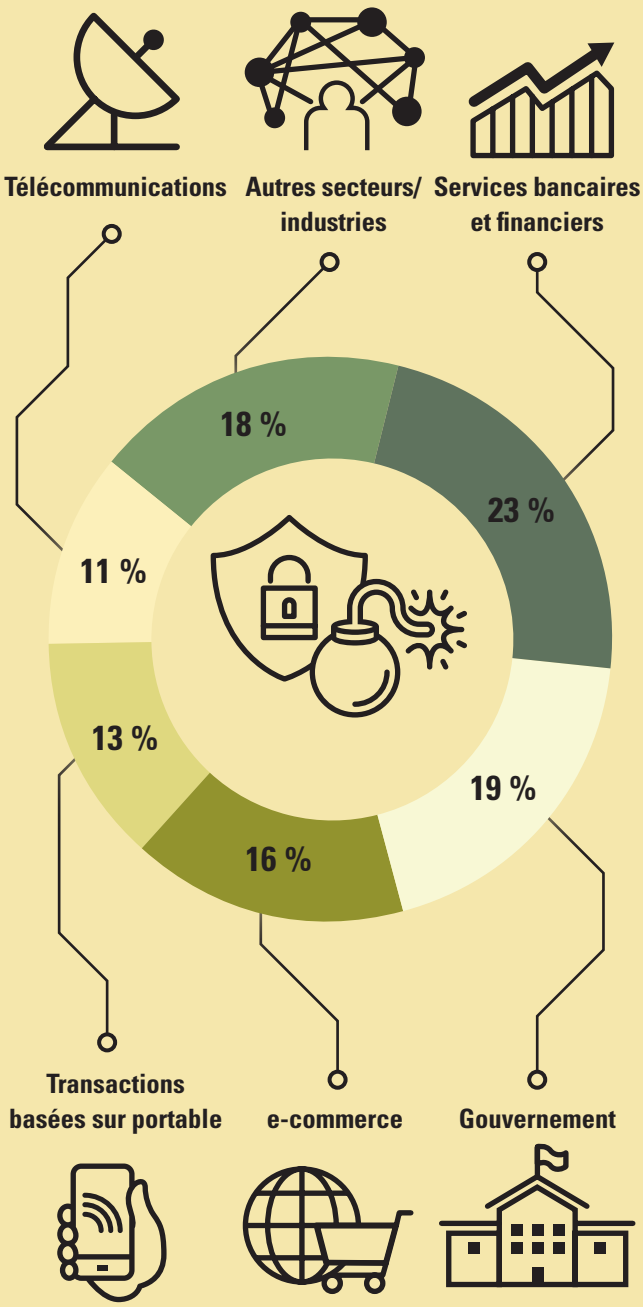


ILLUSTRATION D'*ADF*

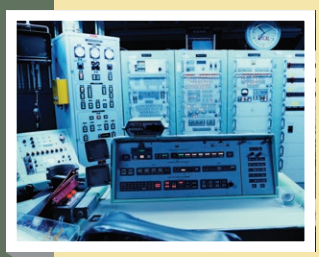
Source: Serianu

Comment les attaques cybernétiques affectent la sécurité nationale

Les attaques cybernétiques deviennent une tactique préférée de ceux qui aiment attaquer à distance et à un coût relativement faible. Les groupes tels que les gouvernements étrangers hostiles, les activistes, les terroristes et les criminels utilisent désormais ces tactiques. « La menace des attaques cybernétiques prend pied en Afrique, mais les gouvernements et le secteur privé n'ont pas encore investi dans des défenses adéquates pour endiguer leur propagation », déclare William Makatiani, PDG de la société kényane de cybersécurité Serianu. « La sécurisation des données devrait donc être une priorité pour les institutions publiques et privées compte tenu de l'évolution rapide des menaces. »

Infrastructure critique :

Les réseaux électriques, les systèmes d'alimentation en eau et les égouts, les métros, les barrages et même les centrales nucléaires ont été ciblés par les attaques cybernétiques. Dans de nombreuses régions du monde, cette infrastructure est gérée par des systèmes obsolètes et elle est particulièrement vulnérable face aux hackers. Exemple : l'attaque de décembre 2015 sur le réseau électrique ukrainien. Selon les rapports, les attaquants ont utilisé un e-mail de hameçonnage pour gagner l'accès au réseau électrique et provoquer une panne de courant ayant affecté 230.000 personnes.



Systèmes d'armement :

Les systèmes d'armement modernes sont équipés de logiciels essentiels embarqués et utilisent la technologie de l'information. Cela peut inclure des systèmes de ciblage utilisés pour tirer les missiles, des logiciels de vol et des mécanismes de lancement d'armes. Bien que cette connectivité offre des perfectionnements en temps de guerre, elle laisse aussi ces systèmes vulnérables face aux intrusions et aux perturbations des adversaires.

Institutions financières :

Les banques sont les cibles les plus fréquentes des attaques cybernétiques. Dans certaines attaques, les criminels utilisent un maliciel ou d'autres méthodes pour gagner l'accès aux informations stockées telles que les numéros de carte de crédit, les identifiants de connexion et les numéros d'identité fournis par l'état. D'autres attaques visent à refuser le service et à causer des pannes de système. La capacité d'un serveur peut être dépassée par des demandes simultanées, ce qui peut le paralyser. En 2017 au Kenya, les clients de M-Shwari, service bancaire sur portable, ont été privés d'accès à leur compte pendant cinq jours. Lorsque l'accès a été rétabli, certaines personnes ont indiqué qu'il leur manquait des fonds.

Agences gouvernementales :

Les bureaux de l'état représentent une cible attractive pour les cybercriminels. Certains attaquants utilisent un logiciel de rançon pour prendre le contrôle des autres sites d'état ; d'autres veulent voler les informations confidentielles ou secrètes du gouvernement. Parfois, le but est une déclaration politique. Un hacker notoire d'Afrique du Sud a pris le contrôle des sites Internet de la Présidence, du Trésor, du Centre de cybersécurité et du ministère des Affaires environnementales pour afficher des messages politiques.

Le circuit de la sécurité

La protection contre la cybercriminalité nécessite une préparation, une vigilance et une réponse rapide. Les experts en sécurité déclarent qu'il est utile de penser à un circuit de la cybersécurité, dans lequel chaque élément de la préparation est lié au suivant. En élaborant et en maintenant ce circuit, les organismes de toute taille peuvent se protéger contre les attaques.

ILLUSTRATION D'*ADF*

Source : Adaptation d'une politique cybernétique utilisée par l'organisation maritime internationale BIMCO

ILLUSTRATION D'*ADF*

QUI DÉFEND LE WEB ?

LES FORCES ARMÉES CRÉENT DES COMMANDEMENTS CYBERNÉTIQUES MAIS LEUR RÔLE EST TOUJOURS DÉBATTU

PERSONNEL D'*ADF*

Historiquement, les avancées technologiques et les nouvelles découvertes ont conduit à la restructuration des armées. Huit ans après le premier vol aérien, des avions furent utilisés dans les combats de la Première Guerre mondiale. Peu de temps après, les premières armées de l'air furent créées. De même, l'introduction des sous-marins conduisit à la guerre sous-marine, et la navigation spatiale suscita des discussions sur la façon de défendre l'espace.

Les forces armées se sont toujours adaptées à l'évolution de la menace. Le cyberespace constitue leur plus récent défi.

En principe, les forces armées sont chargées de défendre le pays contre les menaces extérieures, alors que la police et les autres agences de sécurité s'occupent des questions intérieures.

Mais les menaces cybernétiques sont à la fois extérieures et intérieures. Les attaques peuvent être lancées depuis un lieu quelconque de la planète et peuvent infecter les systèmes d'information du pays. Les attaquants peuvent être des états, des terroristes, de petits délinquants ou des activistes. Les solutions à ce problème varient mais presque tous les pays conviennent que les forces armées ont un rôle à jouer.

« Les conséquences potentielles d'une attaque cybernétique majeure, en ce qui concerne les dommages subis par l'économie et la capacité de fonctionnement du pays, sont telles que ces attaques devraient être considérées dans le cadre de la défense », déclare l'analyste de défense sud-africain Helmoed Romer Heitman dans un article de defenceWeb. « C'est un domaine fortement basé sur le renseignement, donc les capacités requises de renseignement et de protection/défense et le développement des capacités de préemption et de contre-attaque devraient… exister au sein d'un organisme de défense chargé du renseignement. »

LES ARGUMENTS POUR ET CONTRE

Alors que les forces armées se préparent à jouer un rôle dans la cybersécurité nationale, elles doivent considérer les avantages et les désavantages liés à leur intervention sur ce nouveau champ de bataille.

CAPACITÉ À FOURNIR DE L'AIDE

Le pour : Les forces armées ont en général des ressources importantes et sont axées sur la mission. Dans les pays moins développés, les forces armées pourraient être la seule institution capable de mobiliser des ressources contre une menace cybernétique importante.

Le contre : Si les forces armées dirigent la cybersécurité, cela pourrait évincer le secteur privé et freiner son développement dans ce domaine.

CELA S'INSCRIT DANS LA MISSION

Le pour : La cybersécurité est liée à la mission de défense du territoire contre les adversaires extérieurs.

Le contre : La poursuite de tous les cas de cybercriminalité peut excéder les ressources des forces armées et provoquer des accusations selon lesquelles elles outrepassent leur mandat juridique.

INFRASTRUCTURE CRITIQUE

Le pour : Les attaques contre l'infrastructure critique telle que les réseaux électriques et le contrôle du trafic aérien peuvent paralyser un pays. Les forces armées ont le devoir d'assurer une protection contre ces attaques.

Le contre : La défense des réseaux cybernétiques qui contrôlent l'infrastructure critique nécessite une expertise spéciale. Les experts cybernétiques employés par le secteur privé ou par les gouvernements locaux ou ceux qui participent à une équipe de réponse aux urgences informatiques sont mieux aptes à étudier et à protéger ces réseaux.

OFFENSIVE

Le pour : Les attaques cybernétiques militaires offensives peuvent frapper les adversaires avant qu'ils n'attaquent. Dans certains cas, ces attaques peuvent perturber les programmes d'armement de l'ennemi ou endommager son infrastructure.

Le contre : La militarisation de l'Internet pourrait provoquer l'intensification du conflit et conduire à des représailles.

« SI VOTRE PAYS SUBIT UNE ATTAQUE CYBERNÉTIQUE TOTALE ET SOUTENUE CONTRE LES INSTITUTIONS CLÉS, VOUS VOUDREZ MOBILISER TOUS LES ASPECTS DU POUVOIR NATIONAL, Y COMPRIS LES FORCES ARMÉES. »

– Ian Wallace
co-directeur de l'initiative de cybersécurité de la New America Foundation

Dans beaucoup de pays, l'armée a un avantage en termes de ressources et de savoir-faire, ce qui en fait une candidate naturelle pour assurer la protection contre la cybercriminalité. L'Afrique du Sud et le Nigeria ont créé des commandements cybernétiques autonomes et beaucoup d'autres pays africains renforcent leur formation et leurs capacités au sein des structures de commandement existantes.

Dans cette perspective, il est important d'examiner les rôles que les forces armées peuvent assumer et les limites de ce qu'elles peuvent accomplir pour affronter la menace cybernétique.

1. LA PROTECTION DES COMMUNICATIONS ET DU MATÉRIEL MILITAIRE

Dans la plupart des pays, les forces armées sont chargées du renseignement d'origine électromagnétique et utilisent un éventail d'équipements de communication tels que les téléphones et les radios par satellite. Le matériel et l'armement de la défense deviennent plus perfectionnés et dépendent de plus en plus des systèmes d'information. Les systèmes mondiaux de positionnement peuvent effectuer tous les pistages, depuis les bombes jusqu'aux jeeps et aux combinaisons en kevlar. La perturbation de ce flux d'information serait catastrophique.

« La capacité de protéger ces systèmes devient absolument essentielle », déclare Ian Wallace, co-directeur de l'initiative de cybersécurité de la New America Foundation. « Pas nécessairement parce qu'on pourrait être empêché d'utiliser efficacement ces systèmes, mais aussi parce qu'ils pourraient être pénétrés par des adversaires pour saisir leurs informations ou même pour duper. »

La pierre angulaire de toute opération de défense cybernétique doit être la protection de son propre matériel et de ses propres informations.

Des véhicules militaires sont présentés lors du salon Egypt Defense Expo au Caire. Les véhicules et les systèmes d'armement modernes possèdent souvent des composants numériques qui les rendent vulnérables aux attaques cybernétiques.
REUTERS

Les forces armées recueillent une vaste quantité d'informations dont l'accès pourrait mettre en péril la vie. Ceci est évident par exemple pour les plans de bataille ou les stratégies de théâtre, mais d'autres informations telles que les dossiers de santé des militaires peuvent être aussi importantes. Lors d'une attaque hypothétique, déclare M. Wallace, des adversaires cybernétiques pourraient accéder aux dossiers de santé des militaires et altérer les types sanguins indiqués de façon à perturber les traitements dans les hôpitaux.

2. LE MAINTIEN D'UNE CAPACITÉ OFFENSIVE

Pour vaincre les menaces cybernétiques, il est nécessaire de perturber les attaques avant qu'elles n'atteignent leur cible. Les professionnels compétents peuvent atteindre la source d'une menace et la dégrader plutôt que d'attendre que l'ennemi lance une attaque. Dans une guerre, cette capacité offensive peut aussi être utilisée pour mettre hors service des composantes de l'infrastructure de l'adversaire.

Ceci est une idée controversée puisqu'elle conduit à des accusations selon lesquelles le cyberespace est utilisé à des fins militaires, ce qui pourrait provoquer des ripostes. Mais certains affirment qu'elle est nécessaire. Le lieutenant-colonel Michael Aschmann de la Force nationale de défense d'Afrique du Sud a co-écrit un article précisant pourquoi, selon lui, les pays africains doivent investir dans les « armées cybernétiques ».

« L'armée cybernétique [le commandement cybernétique] d'un état-nation africain sera une extension de la puissance militaire du pays, qui lui permettra de combler l'écart avec la cinquième dimension, la sphère de l'info, écrit le lieutenant-colonel Aschmann. Elle améliorera la défense et la protection du secteur technologique et du cyberespace du pays, et elle pourra passer à l'offensive pour contrer l'attaque cybernétique d'un adversaire. »

Cette capacité fait toujours ses premiers pas dans de nombreux pays. Les débats concernant les conditions de son utilisation sont animés.

3. LA PROTECTION DE L'INFRASTRUCTURE CRITIQUE

Une attaque cybernétique sur l'infrastructure critique d'un pays peut paralyser ce dernier. Les éléments tels que les routes et les ponts, la production d'énergie, le transport aérien commercial, l'eau et les systèmes de santé sont cruciaux pour la défense nationale.

C'est pourquoi les forces armées doivent être prêtes à répondre à une attaque cybernétique massive contre l'infrastructure critique. Toutefois, M. Wallace met en garde contre

LE NIGERIA CRÉE LE PREMIER CYBER-COMMANDEMENT D'AFRIQUE

PERSONNEL *D'ADF*

Le Nigeria est l'un des pays africains les plus proactifs dans la lutte contre la cybercriminalité, ce qui est tout à fait justifié. La Commission des communications du Nigeria déclare que le pays détient mondialement la troisième place pour les cybercrimes, derrière le Royaume-Uni et les États-Unis.

Les organisations nigérianes sont ravagées par les logiciels de rançon, les fraudes liées à la cryptomonnaie, les systèmes de Ponzi cybernétiques et d'autres crimes. Les virus informatiques existent couramment depuis des années. L'étendue du problème n'est pas connue car il est estimé que 80 % des cybercrimes au Nigeria ne sont pas déclarés.

La loi nigériane de 2015 sur la cybercriminalité impose des sentences allant jusqu'à la peine de mort en cas de condamnation pour cybercrime.

Les forces armées du pays décidèrent en 2016 de faire face à la cybercriminalité, mais ce fut seulement en août 2018 que le commandement de la guerre cybernétique fut créé, avec des effectifs initiaux de 150 soldats provenant de l'armée régulière et formés en technologie de l'information. Leur mission consiste à surveiller et à défendre le cyberespace, et à attaquer les cybercriminels.

En février 2019, le lieutenant-général Tukur Buratai du Nigeria déclare : « J'ai ordonné au commandement de la guerre cybernétique de l'armée nigériane de perturber les activités de propagande des terroristes en créant des récits de riposte robustes pour neutraliser les efforts visant à tromper et à représenter faussement la situation sur le terrain. »

Le général Buratai déclare que la guerre cybernétique est le cinquième secteur de la guerre, après les secteurs terrestre, maritime, aérien et spatial. Il affirme qu'il représente la forme la plus dangereuse.

Le chef d'état-major de l'Armée de terre du Nigeria, lieutenant-général Tukur Buratai. REUTERS

« Les caractéristiques intrinsèques du cyberespace peuvent être facilement exploitées aux fins de la guerre de l'information par des acteurs ayant de mauvaises intentions pour désinformer et diffuser des informations fallacieuses, et pour demander à des utilisateurs rémunérés de propager un contenu manipulé en ligne », déclare le général Buratai selon un reportage du journal nigérian *Leadership*.

Le général Buratai déclare qu'il a affecté au commandement la tâche routinière d'étudier et d'analyser les activités suspectes en ligne pour aider les forces armées à devenir proactives dans leur traitement des cybercrimes. Africa Independent Television signale que ce commandement traitera des questions telles que le cyberterrorisme, la propagande extrémiste, les efforts de recrutement des terroristes, les informations malicieuses et le vol des données. « Il améliorera aussi la surveillance numérique de toutes les opérations en cours, en particulier la guerre contre Boko Haram dans le Nord-Est du Nigeria », signale la chaîne.

Le quartier général provisoire du commandement sera situé à Abuja, avec des antennes régionales créées selon les besoins. La construction d'un complexe de bureaux permanent a été autorisée. Le Nigeria a aussi conduit des discussions avec l'Afrique du Sud pour travailler conjointement contre la cybercriminalité.

POUR PROTÉGER L'INFRASTRUCTURE CRITIQUE, DE NOMBREUX PAYS ORGANISENT DES ÉQUIPES DE RÉPONSE AUX URGENCES INFORMATIQUES RÉUNISSANT DES EXPERTS DANS PLUSIEURS DOMAINES.

l'utilisation des forces armées comme première ligne de défense dans ce domaine.

« Si votre pays subit une attaque cybernétique totale et soutenue contre les institutions clés, vous voudrez mobiliser tous les aspects du pouvoir national, y compris les forces armées », déclare-t-il.

Mais demander aux forces armées de diriger la défense contre les nombreux incidents cybernétiques de moindre importance qui se produisent régulièrement peut provoquer deux types de problème. Premièrement, les forces armées pourraient évincer le secteur privé en freinant le développement de la cybersécurité dans ce secteur. Deuxièmement, les forces armées pourraient assumer un fardeau trop lourd qui détournerait les ressources affectées aux autres missions.

M. Wallace recommande une approche consistant à « verrouiller sa propre porte », dans laquelle le secteur privé, soutenu par la police, dirige les réponses contre la plupart des attaques cybernétiques. Les forces armées seraient mobilisées uniquement comme dernière ligne de défense pour déjouer une attaque majeure.

« Étant donné l'omniprésence des systèmes d'information dans l'ensemble de la société, si les forces armées étaient seules responsables de la défense de ces systèmes, elles s'introduiraient dans de nombreux secteurs de la société où il est probablement préférable qu'elles ne s'introduisent pas, pour le bien du pays et pour le bien des forces armées », déclare M. Wallace.

Pour protéger l'infrastructure critique, de nombreux pays organisent des équipes de réponse aux urgences informatiques (CERT) réunissant des experts dans plusieurs domaines. Ces spécialistes, souvent appuyés par un financement gouvernemental, ont des connaissances approfondies des systèmes nationaux critiques et peuvent jouer le rôle de premiers intervenants après une attaque ou une activité suspecte.

Le Dr Benoît Morel, expert en technologie de l'information et de la communication, affirme que les pays africains ont particulièrement besoin de développer des CERT. Il mentionne le Maroc et l'Égypte comme exemples d'histoire à succès. « Les pays africains ne devraient pas attendre. Ils devraient développer leur expertise chez eux, dès maintenant, écrit le Dr Morel. Pour le moment, les meilleurs experts en cybersécurité sont en général les cybercriminels. En Afrique, le développement de ce type d'expertise au niveau local se traduira par des actions qui seront différentes de celles entreprises par les économies développées. Un noyau d'expertise doit être développé… un groupe de personnes (qui n'ont pas besoin d'être très nombreuses), dont la mission consiste à assumer la responsabilité de la cybersécurité dans le pays. » ❑

Le terminal portuaire à Alger (Algérie). Les adversaires cybernétiques prennent pour cible l'infrastructure nationale critique, et certaines forces armées s'entraînent pour la protéger.

REUTERS

Le développement grâce à la numérisation

Le conseiller en cybersécurité du Ghana déclare que le pays se prépare pour les opportunités et les menaces du monde du numérique

MINISTÈRE DES COMMUNICATIONS DU GHANA

Depuis 2017, le Dr Albert Antwi-Boasiako est conseiller national en cybersécurité du gouvernement du Ghana. Il est aussi le fondateur de l'e-Crime Bureau, société panafricaine de cybersécurité et de science forensique. L'e-Crime Bureau a travaillé avec la police, les forces armées et les organismes privés et publics à travers le continent. Il a créé le premier labo de cybersécurité et de science forensique numérique d'Afrique de l'Ouest. Cette interview a été modifiée pour l'adapter à ce format.

ADF : **Dans votre rôle actuel de conseiller national en cybersécurité, vous aidez à élaborer la politique de cybersécurité du Ghana. Quelles sont les principales menaces auxquelles le Ghana fait face dans ce domaine ?**

Dr Antwi-Boasiako : J'ai peur d'une attaque cybernétique qui ciblerait l'infrastructure nationale critique de l'information. C'est le problème le plus difficile. C'est ce qui me force à réfléchir, ce qui m'empêche de dormir : une attaque qui saperait nos systèmes critiques d'information. Au Ghana, la fraude cybernétique, l'imposture, le vol d'identité et la fraude commerciale sont très répandus. Toutefois on peut vivre avec cela. Ces choses sont signalées, et une certaine réponse est mise en œuvre. Mais ce qui pourrait vraiment saper notre pays en voie de développement, [c'est un type différent d'attaque]. Je soulève cette idée parce que le gouvernement a ce que l'on appelle un programme du « Ghana au-delà de l'aide ». C'est une structure et une direction politique du gouvernement, avec un très grand élément de numérisation. Le gouvernement veut assurer le développement grâce à la numérisation. Beaucoup d'initiatives ont été déployées. Nous avons des ports sans papier : les ports, les services de douane, les importations, les exportations sont réalisés sur une plateforme en ligne. Le gouvernement déploie aussi un système d'identification national dans l'ensemble du pays. Nous venons de lancer le système e-Justice dans lequel l'administration de la justice est livrée électroniquement. Nous avons lancé un système national d'adressage des propriétés immobilières. J'appelle tout cela des « initiatives de numérisation du gouvernement » et, de concert avec l'infrastructure nationale critique de l'information, elles constituent un secteur important de notre économie. La peur d'une attaque cybernétique, c'est la peur qu'elle affecterait la sécurité nationale et qu'elle éroderait la confiance que nous établissons en termes de cybersécurité.

ADF : **Quel est le secteur le plus ciblé ?**

Dr Antwi-Boasiako : Nous avons subi un certain nombre d'attaques visant l'infrastructure nationale critique de

La Banque du Ghana et le reste du secteur financier du pays s'efforcent de renforcer la cybersécurité.

REUTERS

l'information dans le secteur financier. En fait, plus de 70 % des attaques que nous subissons ont des motifs financiers. Des systèmes sont compromis ; on essaie de retirer l'argent des comptes des clients. Le gouvernement a pris l'initiative d'établir des systèmes de sécurité à la Banque du Ghana pour faire face au problème. Une nouvelle directive sur la cybersécurité financière a été introduite pour assurer que les institutions financières accroissent leurs efforts en cybersécurité. Ces mesures sont déployées dans les secteurs de l'infrastructure nationale critique de l'information. Elles répondent directement à la peur que nos ressources critiques d'information pourraient être ciblées par une attaque cybernétique.

ADF : **Le Ghana est devenu un chef de file régional et continental en cybersécurité. Le pays lance un Centre national pour la cybersécurité. Quel rôle jouera ce centre dans l'amélioration de la cybersécurité ?**

Dr Antwi-Boasiako : La cybercriminalité est une question interdisciplinaire. C'est un problème multidimensionnel. Il y a donc différentes agences publiques et privées dont le rôle ou le mandat est associé à la cybersécurité. Pour affronter un problème de ce type, il faut établir un point de contact central. Le Centre national pour la cybersécurité a donc été établi pour coordonner les activités liées à la cybersécurité au sein du gouvernement et dans le secteur privé. Parmi ses fonctions principales, on compte la réponse aux incidents, la génération de la sensibilisation, les contacts avec le Parlement, la fourniture des conseils et le développement des meilleures pratiques. En ce qui concerne la mise en œuvre, nous en sommes au niveau formatif. Nous ne sommes plus au stade du démarrage, mais nous sommes toujours en formation. Cela veut dire que nous avons pu recruter une équipe et que nous travaillons activement au développement de la sensibilisation. Nous déployons la technologie pour faciliter le partage des informations sur les menaces et les incidents cybernétiques, pour les diffuser auprès de toutes les parties prenantes. Cela veut dire qu'elles pourront signaler les incidents, et aussi recevoir les informations distribuées par le centre sur les menaces.

Le président ghanéen Nana Akufo-Addo s'exprime à Accra au début du Mois de la sensibilisation nationale à la cybersécurité.

MINISTÈRE DES COMMUNICATIONS DU GHANA

ADF : **Le ministère des Communications du Ghana a établi un partenariat avec le Centre international de formation de maintien de la paix Kofi Annan afin de créer un laboratoire de formation pour les professionnels de la sécurité. Est-il important selon vous que des membres des forces armées et de la police soient formés en cybersécurité ? Quel est le rôle que les forces armées devraient jouer dans la cybersécurité ?**

Dr Antwi-Boasiako : En ce qui concerne l'architecture nationale de la cybersécurité, les forces armées sont un acteur important. Nous parlons essentiellement de la défense cybernétique qui doit être intégrée dans la formation militaire. Il est aussi important de noter qu'il existe un changement de paradigme et que les mesures nécessaires doivent être prises pour intégrer la cyber-défense dans le programme de formation, dans la réflexion, dans la stratégie et dans la politique de l'environnement militaire. L'e-Crime Bureau a donc créé une relation avec le Centre international de formation de maintien de la paix Kofi Annan. Un labo a déjà été établi. Il contient 32 ordinateurs équipés de technologie, d'outils de piratage, d'outils forensiques et de programmes de formation. La formation se fait à deux niveaux. Le premier est la création de la sensibilisation parmi les hommes et les femmes en uniforme et les officiers de maintien de l'ordre pour qu'ils apprécient les dangers des problèmes cybernétiques afin de pouvoir diriger les actions militaires sur le renforcement des capacités et la recherche et le développement. Le deuxième concerne des programmes de formation visant à introduire les outils cybernétiques offensifs et défensifs aux officiers militaires versés dans la technologie, simplement pour qu'ils se familiarisent avec ce nouveau domaine. Toute force militaire souhaitant rester pertinente doit adopter cela et développer ses aptitudes. Je crois que les capacités cybernétiques militaires se développent spectaculairement dans notre région. Je recommande au gouvernement de développer une stratégie de défense qui intègre efficacement la cybersécurité à la protection des données, des systèmes et des réseaux des forces armées, et qui prépare aussi nos soldats à protéger et à défendre le pays. Les attaques sont lancées par des étrangers qui tentent vraiment de porter atteinte à notre pays et de le détruire. Les forces armées doivent assumer un rôle lié à des mesures préventives et des mesures défensives.

ADF : **Le Ghana crée des équipes de réponse aux urgences informatiques (CERT) pour faire face aux incidents cybernétiques. Quel sera le rôle de ces CERT pour protéger le pays contre les attaques cybernétiques et pour répondre rapidement en cas d'attaque ?**

Dr Antwi-Boasiako : La CERT nationale a été établie au sein du Centre national pour la cybersécurité. Le Ghana utilise un système de CERT décentralisé. « Décentralisé » veut dire que l'on a identifié certains secteurs critiques. Les forces armées en sont un, le secteur financier en est un autre, et aussi le gouvernement, les télécommunications, l'énergie et l'environnement académique. Chacun de ces secteurs travaille sur une CERT qui agit en coordination avec la CERT nationale. Ainsi, nous avons par exemple déjà créé la CERT du secteur des télécommunications. L'Autorité nationale des communications, qui est l'organe régulateur et détient l'autorité pour la sécurité des systèmes critiques dans l'environnement des télécommunications, supervise cela. Le secteur financier a créé une CERT pour protéger les dispositifs et les réseaux de ce secteur, et cette CERT est aussi liée à la CERT nationale. La CERT nationale détient un rôle de coordination plus vaste tandis que les CERT sectorielles sont chargées des systèmes, réseaux et données au sein de leur secteur particulier. Ceci fonctionne dans l'ensemble, et nous avons des

Une illustratrice parle à un client à Accra (Ghana). Avec la croissance du commerce numérique, le pays s'efforce d'améliorer la cybersécurité. REUTERS

pays d'Afrique de l'Ouest qui viennent ici pour tirer des leçons de l'exemple du Ghana.

ADF : **Beaucoup de pays, notamment certains pays d'Afrique de l'Ouest, ont des ressources limitées. Comment devraient-ils prioriser la cybersécurité ?**

Dr Antwi-Boasiako : J'estime que, au cours des 50 prochaines années, la question du manque de ressources ou du manque de financement ne sera pas reléguée au passé. Elle restera une question d'actualité en Afrique. Si nous décidons qu'il faut avoir de l'argent pour obtenir des résultats, nous n'y arriverons jamais. C'est une question d'intelligence pragmatique. Nous devons nous la poser ainsi : Notre développement est-il lié à la numérisation ? Comment les économies africaines peuvent-elles se développer sans passer au numérique ? Ce serait impossible. Nous serions en fait coupés du reste du monde. Je crois que l'argument proposé par le Ghana est qu'il n'existe pas d'alternative à la numérisation. Les Nations unies et la Banque mondiale ont estimé qu'elle a le potentiel de transformer notre économie. L'e-commerce crée des emplois sur le continent. Donc, pour tout pays africain visionnaire, la numérisation est la clé, et par conséquent des mesures doivent être prises pour assurer que les investissements dans le développement de la technologie de l'information et des communications soient protégés. Le gouvernement du Ghana a résolu d'établir un fonds de cybersécurité parce que le développement de la cybersécurité du pays ne peut pas être durable s'il est soutenu par les donneurs. Notre président veut construire le « Ghana au-delà de l'aide » et nous devons être innovateurs. Vers la fin de l'année, le gouvernement va établir un fonds de cybersécurité pour développer l'écosystème de la cybersécurité. Et j'ai conseillé de rechercher des façons innovantes d'obtenir les fonds nécessaires pour engager du personnel dans les secteurs de la justice criminelle, de la défense et du gouvernement, ainsi que dans le secteur privé et dans celui de la société civile. De cette façon, ils pourront obtenir ces écosystèmes cybernétiques résilients pour que nos investissements en numérisation soient protégés. ❑

Un peintre ivoirien redonne vie aux déchets électroniques

REPORTAGE ET PHOTOS PAR REUTERS

Désiré Koffi marche souvent dans Koumassi, district de la classe ouvrière d'Abidjan (Côte d'Ivoire), pour acheter de vieux téléphones portables à un coût de 500 francs CFA (0,87 dollar) les deux.

Lorsqu'il rentre chez lui, cet artiste de 24 ans fracasse les téléphones à coups de marteau et en retire les écrans et les claviers. Il les utilise pour ses peintures, dont l'exécution peut prendre entre trois et cinq jours.

M. Koffi a passé son enfance à Koumassi et déclare qu'il a été attiré par le recyclage et l'utilisation des déchets électroniques dans ses peintures après avoir vu comment les déchets affectaient son environnement.

« Mon objectif numéro un est d'essayer, avec mes modestes moyens, de réduire les déchets électroniques que l'on trouve dans les rues et dans les poubelles, déclare-t-il. Nous sommes ici dans l'un des quartiers les plus populaires de la ville, où on trouve en général de vieux téléphones qui ne peuvent plus être réparés. »

Avec une population de 5,5 millions, Abidjan accumule jusqu'à 1.500 tonnes de déchets électroniques par an, selon E-waste Implementation Toolkit [Boîte à outils de mise en œuvre des déchets électroniques]. M. Koffi déclare qu'une grande partie de ces déchets peuvent être utilisés pour gagner de l'argent.

Ayant participé à plusieurs expositions à l'étranger et dans son pays, M. Koffi est rapidement en train de devenir l'une des plus importantes personnalités de Côte d'Ivoire en art contemporain.

« Je pense que son travail est excellent. Il a décidé de faire du recyclage, et cela lui va très bien parce que son travail se distingue de tous les autres », déclare Ézéchiel Guibe, un autre artiste ivoirien.

« Bien qu'il intègre du matériel recyclé dans ses œuvres, il réussit à capturer toutes ces formes, ces visages et ces émotions dans son travail, ce qui nous a vraiment émerveillé », déclare Olivier Pépé, directeur d'une galerie d'art.

LES MENACES PROLIFÈRENT À MESURE QUE LE CONTINENT DEVIENT CONNECTÉ

ILLUSTRATION *ADF*

La croissance de l'Internet en Afrique s'accompagne d'une augmentation des risques et des opportunités

PERSONNEL D'*ADF*

La possibilité d'attaques cybernétiques paralysantes n'est plus le domaine de la science-fiction ou des films à gros budget. Les outils de la guerre cybernétique ont été mis à l'épreuve sur une grande et une petite échelle dans le monde entier.

En bref, les attaques cybernétiques ne vont pas disparaître. L'exemple le plus important et le plus connu est peut-être celui de l'Ukraine. C'était là, en décembre 2016, que les lumières se sont éteintes. Des centaines de milliers de résidents ont été plongés dans l'obscurité pendant des heures, jusqu'à ce que des ouvriers puissent réenclencher manuellement le réseau électrique. Une attaque similaire s'était produite un an auparavant. Les pannes d'électricité n'étaient pas des incidents isolés ; au contraire, elles faisaient partie d'une série d'attaques, selon un article de juin 2017 dans le magazine *Wired*.

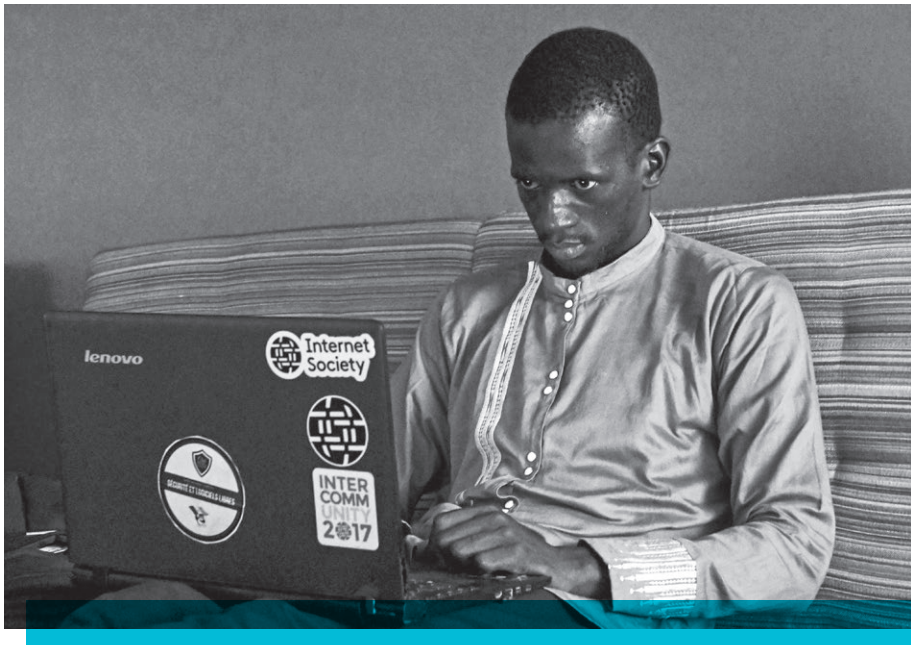
« Elles faisaient partie d'une Blitzkrieg numérique qui s'est acharnée sur l'Ukraine au cours des trois dernières années, un assaut cybernétique soutenu que l'on n'avait jamais vu auparavant, indique *Wired*. Une armée de hackers a systématiquement sapé pratiquement tous les secteurs de l'Ukraine : les médias, le secteur financier, les transports, les forces armées, les organismes politiques, l'énergie. Des vagues successives d'intrusions ont supprimé les données, détruit les ordinateurs et, dans certains cas, paralysé le fonctionnement de base des organisations. »

On suppose que la Russie, qui est de plus en plus connue dans le monde pour ses méfaits cybernétiques, est responsable pour les attaques en Ukraine.

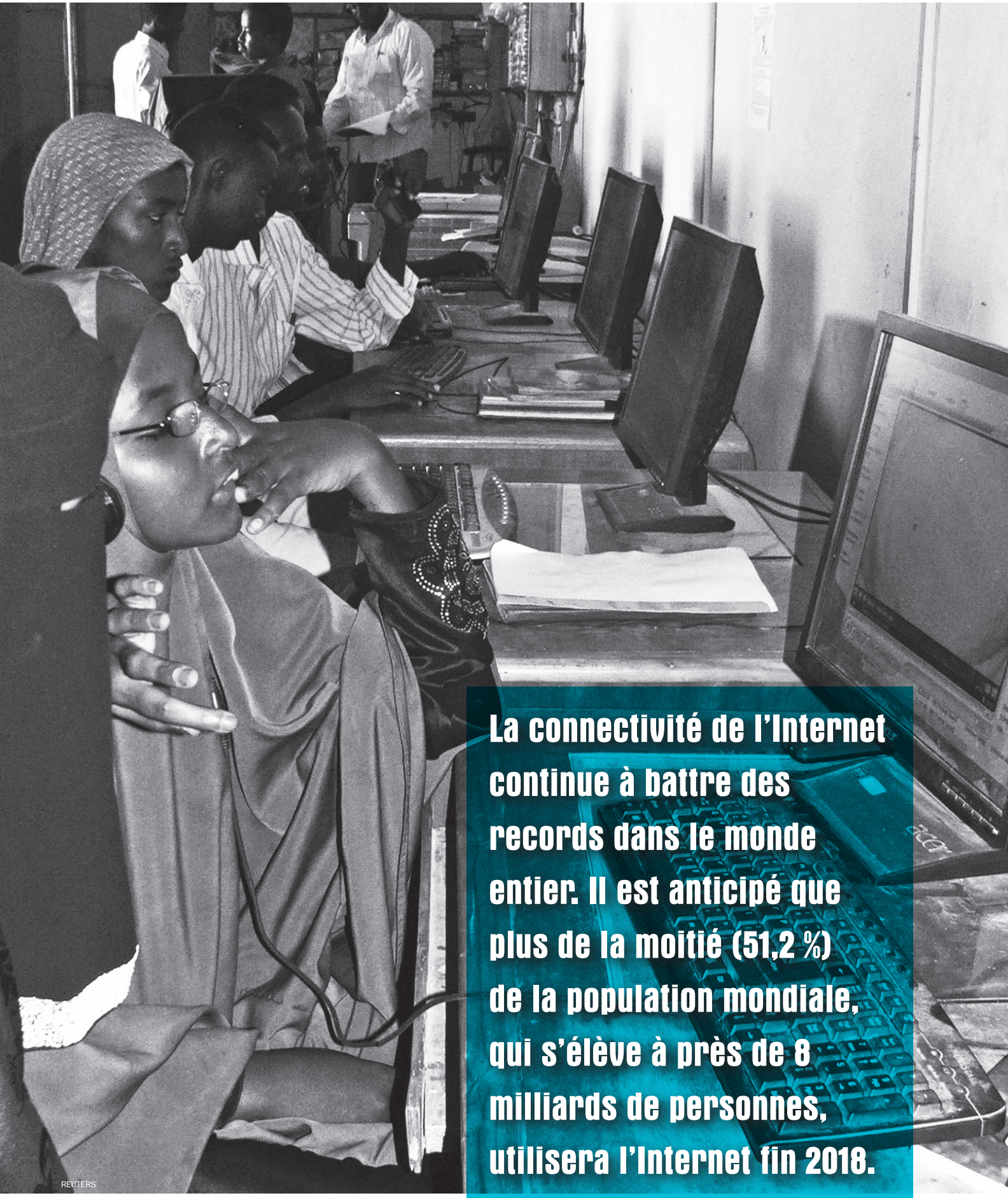
En décembre 2016, le président ukrainien Petro Porochenko déclare que, au cours d'une période de deux mois, il y a eu 6.500 attaques cybernétiques sur 36 cibles en Ukraine. Il en accuse la « participation directe ou indirecte des services secrets de Russie, qui ont lancé une guerre cybernétique contre notre pays », selon *Wired*.

Un grand nombre d'observateurs considèrent que les attaques présumées de la Russie contre l'Ukraine sont une série de tests. Le pays aurait pu aller plus loin et causer plus de dommage pendant plus longtemps, mais il s'est retiré avant de provoquer des dégâts irréparables.

« Ils n'ont pas mis de gants. C'est un lieu où vous pouvez faire le pire sans représailles et sans poursuites judiciaires », a déclaré à *Wired* Kenneth Geers, ambassadeur de l'OTAN qui se spécialise en cybersécurité. « L'Ukraine n'est ni la France ni l'Allemagne. Beaucoup d'Américains ne peuvent pas la trouver sur une carte, donc on peut y faire des tests. »

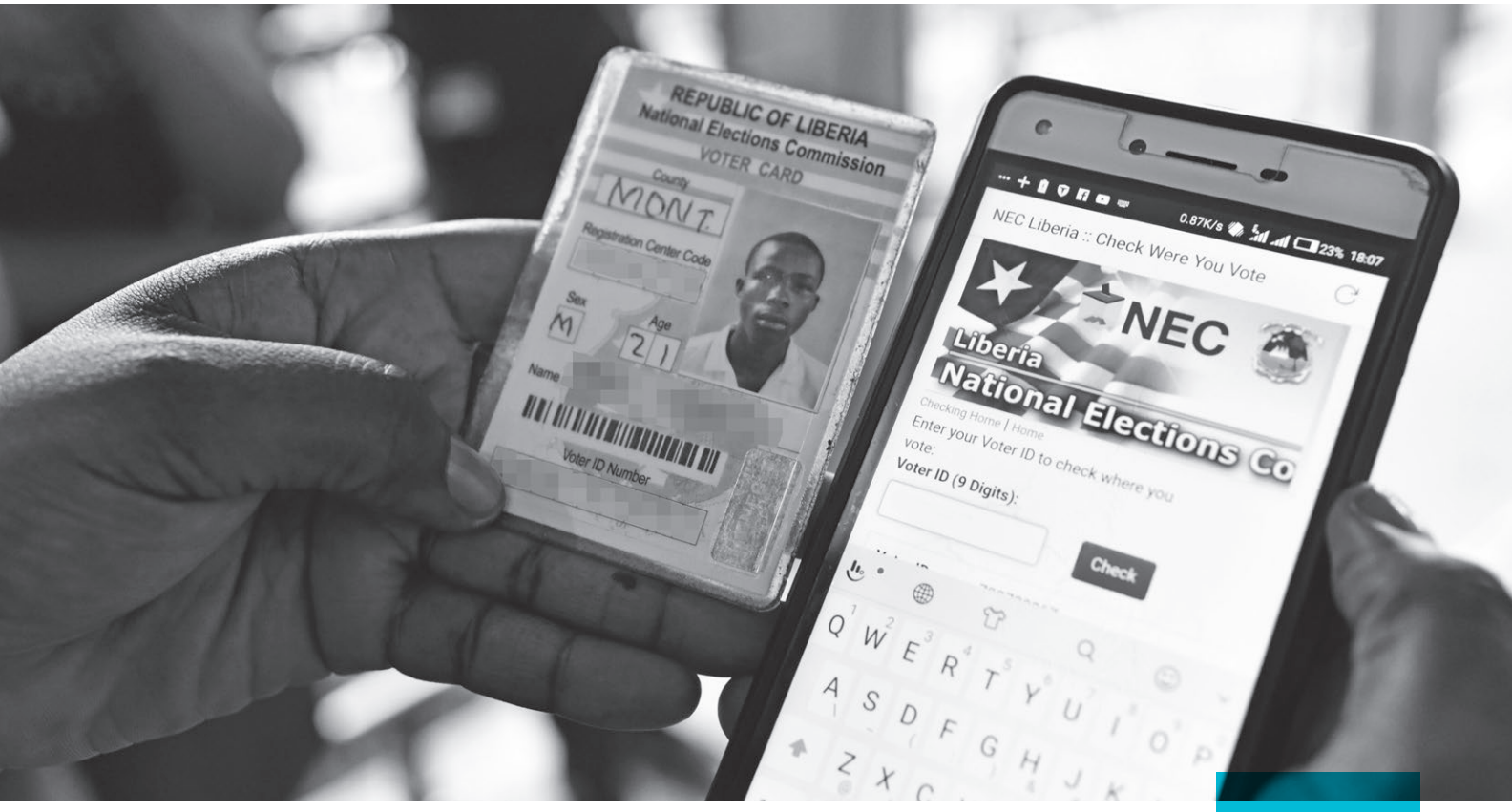


Un homme utilise un ordinateur à Impact Hub Dakar, startup de conception de sites Web au Sénégal. AFP/GETTY IMAGES



La connectivité de l'Internet continue à battre des records dans le monde entier. Il est anticipé que plus de la moitié (51,2 %) de la population mondiale, qui s'élève à près de 8 milliards de personnes, utilisera l'Internet fin 2018.

REUTERS



Un votant libérien vérifie son nom sur le site Web officiel de l'état sur un téléphone portable à l'extérieur d'un bureau de vote.
AFP/GETTY IMAGES

LA MENACE EN AFRIQUE

À première vue, il semblerait improbable que les pays africains fournissent des cibles cybernétiques. Mais cela est certain de changer à mesure que la connectivité augmente sur le continent.

La connectivité de l'Internet continue à battre des records dans le monde entier. Il est anticipé que plus de la moitié (51,2 %) de la population mondiale, qui s'élève à près de 8 milliards de personnes, utilisera l'Internet fin 2018, selon un communiqué de l'agence des télécommunications des Nations unies annoncé en décembre dernier. Les chiffres indiquent aussi que l'Afrique a enregistré la plus forte croissance en accès Internet, allant d'environ 2 % en 2005 à plus de 24 % en 2018, selon le site Modern Diplomacy.

En 2022, il est anticipé que 60 % de l'économie mondiale sera numérisé, selon CNBCAfrica. Et bien que ces améliorations puissent être bénéfiques pour le développement, l'accroissement de la connectivité intensifie les opportunités cybercriminelles. Les attaques cybernétiques provoquent une perte économique annuelle mondiale de 400 milliards de dollars. Les acteurs malveillants ont compromis plus de 4,5 milliards d'archives pendant le premier semestre 2018, soit près du double des 2,7 milliards d'archives compromises pour l'ensemble de 2017.

Le Dr Greg Conti, stratégiste en sécurité pour IronNet Cybersecurity aux États-Unis, déclare qu'il existe deux types principaux d'attaque cybernétique : celles qui sont ciblées et celles qui ne le sont pas. Dans une attaque ciblée, les combattants cybernétiques peuvent décider de compromettre le secteur énergétique ou le réseau électrique d'un certain pays, comme ce qui s'était passé avec les attaques en Ukraine.

Dans une attaque non ciblée, les attaquants cybernétiques peuvent par exemple décider d'attaquer sans distinction tous les barrages du monde. « Si c'est facile, pourquoi ne pas détruire le plus possible ? Cherchez les systèmes vulnérables », déclare le Dr Conti. La détection des vulnérabilités n'est pas aussi difficile que son nom l'indique. Par exemple, un outil appelé Shodan, qui selon CNN est « le moteur de recherche le plus effrayant de l'Internet », cherche les dispositifs connectés à l'Internet 24 h/24, 7 j/7, en recueillant des informations sur 500 millions de services et de dispositifs chaque mois.

Shodan recueille des informations sur tout ce qui existe : depuis le banal (caméras de sécurité, feux rouges et appareils électroménagers) jusqu'au plus sensible, par exemple les systèmes de commandement et de contrôle des centrales nucléaires. CNN indique qu'un grand nombre de ces

Les journalistes nigérians examinent les résultats des élections. Les élections ont été sujettes à des attaques cybernétiques au Nigeria et ailleurs. REUTERS

dispositifs détectés ne bénéficiaient pas de mesures de sécurité.

« Une recherche rapide de "mot de passe par défaut" révèle d'innombrables imprimantes, serveurs et dispositifs de contrôle de système qui utilisent "admin" comme nom d'utilisateur et "1234" comme mot de passe, selon CNN. Beaucoup plus de systèmes connectés n'exigent absolument aucun identifiant de connexion : il suffit d'avoir un navigateur Web pour se connecter à eux. »

Un spécialiste de la sécurité a utilisé Shodan pour trouver une station de lavage qui pouvait être mise en marche et arrêtée, selon CNN. L'ensemble du système de contrôle de la circulation d'une ville, qui était connecté à l'Internet, pouvait être mis dans le mode de test avec une seule commande. S'il est donc aussi facile de scanner tout l'Internet pour rechercher les dispositifs connectés et vulnérables, il est possible que les pays africains deviennent la cible d'une attaque opportuniste généralisée.

« Je dois penser que les acteurs gouvernementaux font des plans à l'avance, déclare le Dr Conti à *ADF*. Si quelque chose est facile à faire, si ce n'est pas dur, je peux imaginer qu'ils attaqueraient l'Afrique et les pays qui ne sont apparemment pas des acteurs de premier plan sur la scène mondiale. »

Les acteurs malveillants donneront priorité à certaines régions, et ils n'ignoreront pas l'Afrique dans leurs calculs. Un rapport du *New York Times* d'octobre 2018 indique que des espions chinois et russes ont écouté les conversations personnelles des leaders mondiaux. Les systèmes de communication des chefs des différentes institutions militaires d'Afrique ont aussi de la valeur. Donc, bien que ces cibles ne méritent pas le même niveau d'effort de la part des hackers soutenus par des gouvernements, elles ne seraient pas immunisées contre les attaques, déclare le Dr Conti.

L'AFRIQUE RÉPOND

Bien que les capacités cybernétiques nécessitent toujours beaucoup de croissance et de développement, un certain nombre de pays africains démontrent une sensibilisation et une préoccupation accrues dans le domaine cybernétique.

L'Afrique du Sud a entrepris une stratégie offensive en 2016 et créé une équipe de réponse aux incidents de cybersécurité « pour empêcher ou surmonter un incident

Une banque et un cybercafé nigérians sont représentatifs de la croissance de la connectivité dans toute l'Afrique. REUTERS

de guerre cybernétique grâce à la création du centre de commandement cybernétique », selon OIDA Strategic Intelligence, cabinet français indépendant d'intelligence économique. Cette équipe publie des conseils et des rapports en matière de sécurité de l'information depuis au moins octobre 2018.

Le Nigeria est aussi proactif pour affronter les menaces cybernétiques. L'Arméenigériane a créé un commandement de guerre cybernétique, qui sera censé employer 150 personnes provenant des forces armées qui seront formées dans la technologie de l'information, selon un rapport de *Forbes*. L'objectif du commandement est de « surveiller, défendre contre et attaquer en cyberespace par des attaques distribuées de type "refus de service" les criminels, les états-nations et les terroristes ». Le Nigeria a subi un grand nombre d'attaques cybernétiques, notamment celle qui a piraté le site Internet de la Commission électorale nationale indépendante pendant l'élection de 2015, et pour laquelle il accuse le groupe d'insurgés Boko Haram.

Le ministère des Communications du Ghana a établi le Centre national pour la cybersécurité qui est chargé de coordonner les activités de cybersécurité du gouvernement et du secteur privé. Il est aussi responsable pour la coordination des incidents de cybersécurité et pour la sensibilisation à ces derniers. Le budget de 2019 de ce pays prévoit la création d'une Autorité nationale pour la cybersécurité, afin de superviser la protection de l'infrastructure nationale critique de l'information, selon Myjoyonline.com.

Le Sénégal a créé l'École nationale de la cybersécurité pour former le personnel du service de sécurité, du secteur judiciaire et du secteur commercial sur la façon de combattre les cybercrimes tels que le financement et la propagande du terrorisme, selon l'Agence France-Presse.

Plus de 1.300 délégués provenant de 28 pays d'Afrique et d'ailleurs se sont réunis pendant deux jours à Nairobi (Kenya) en juillet 2018 lors de la Conférence au sommet inaugurale africaine sur la cyberdéfense. Parmi les participants se trouvaient des représentants gouvernementaux, commerciaux et universitaires provenant de tout un éventail d'industries et de disciplines. Selon ITWeb Africa, Yogida Sawmynaden, ministre de la Technologie, des Communications et de l'Innovation de l'île Maurice, a déclaré aux délégués réunis que l'Afrique nécessitait une loi unique sur la cybersécurité « pour uniformiser nos lois et parler avec un seul langage numérique afin de contrer les attaques ». ❑

L'AFRIQUE

COMBAT LA

CYBER-CRIMINALITÉ

ILLUSTRATION D'A.D.F

À MESURE QUE LE CONTINENT AMÉLIORE SON INFRASTRUCTURE DE COMMUNICATION, IL DEVIENT UNE CIBLE PLUS IMPORTANTE POUR LES CYBERCRIMINELS

PERSONNEL D'*ADF*

Le Maroc et l'Inde, séparés par la culture, la religion, la langue et une distance de 8.458 kilomètres, semblent avoir bien peu en commun. Pourtant, fin 2018, ces deux pays ont signé un protocole d'accord dans le but de coopérer sur plusieurs fronts.

La cybercriminalité est l'un des problèmes que les deux pays partagent. Selon la Commission politique de l'Inde, ce pays occupe le troisième rang mondial parmi les utilisateurs de l'Internet, après les États-Unis et la Chine. L'usage de l'Internet en Inde s'est multiplié par 6 entre 2012 et 2017, soit une croissance annuelle de 44 %. Cette croissance s'est accompagnée d'une hausse de la cybercriminalité : ce pays est classé septième dans le monde pour les envois de spam, et c'est l'un des cinq premiers pour les crimes en ligne.

La police judiciaire du Maroc a enregistré 1.091 cas de cybercrime en 2018, comparé à 765 l'année précédente, soit une augmentation de 33 %. La police du Maroc a signalé 435 victimes du chantage sexuel en ligne, y compris 125 étrangers, et 267 arrestations.

Le protocole d'accord indique que les deux pays vont collaborer sur la cybersécurité. « L'objet du protocole d'accord est d'encourager une coopération plus étroite pour échanger les informations et l'expérience concernant la détection, la résolution et la prévention des incidents liés à la sécurité dans les deux pays, selon une annonce de presse. La mise en œuvre du protocole d'accord conduira à d'importants avantages mutuels dans le secteur de la cybersécurité en Inde, grâce au développement des institutions et des capacités avec le Maroc. »

Le Maroc est l'un des chefs de file africains dans la lutte contre la cybercriminalité. Il exige que les entreprises se conforment aux lois sur le cybercrime, la protection des informations personnelles et les échanges électroniques.

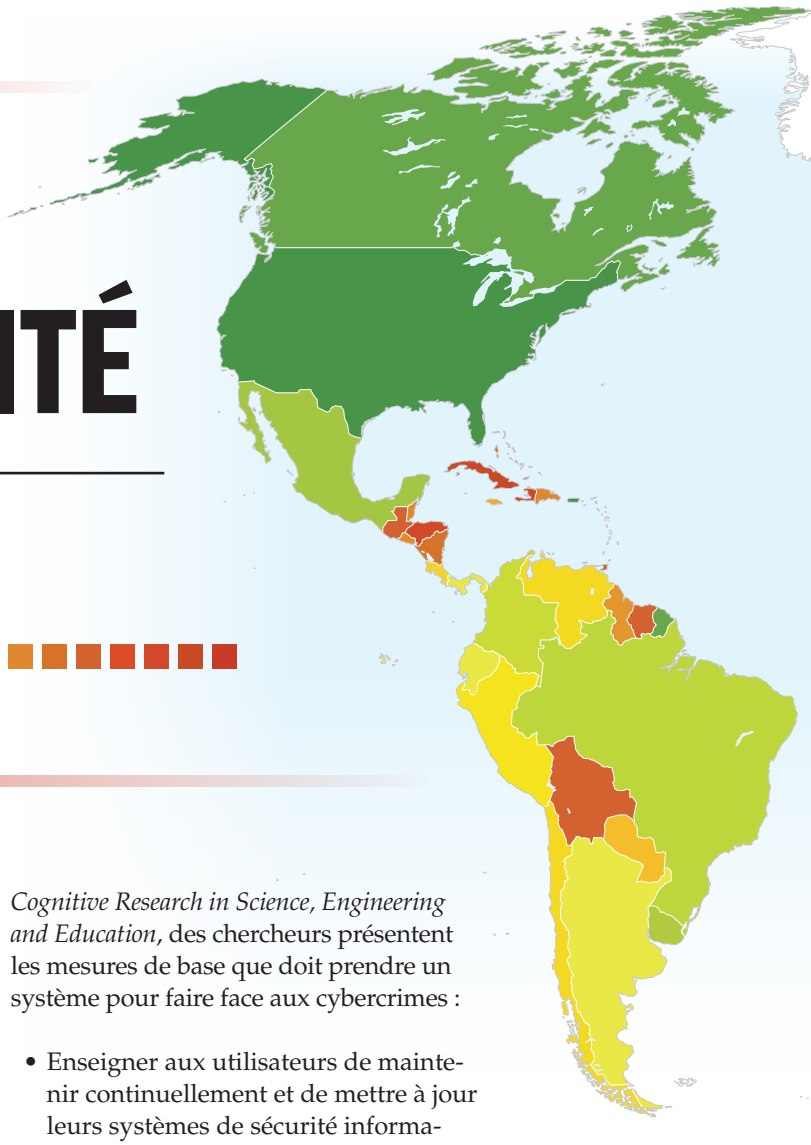
La Brookings Institution basée aux États-Unis déclare que le coût moyen du cybercrime pour les entreprises a augmenté mondialement de 22,7 % depuis 2016. Le détournement des données a augmenté de 27 %. Une seule attaque en mai 2017 par le logiciel de rançon WannaCry a affecté plus de 400.000 ordinateurs dans 150 pays en quelques jours. Début 2019, les responsables des services de renseignement déclarent que le logiciel de rançon WannaCry réside toujours sur des centaines de milliers d'ordinateurs, bien qu'il soit dans un état de dormance.

> « CE N'EST PAS UNE EXAGÉRATION DE DIRE QUE **80 % DE TOUS LES ORDINATEURS** QUI SE TROUVENT EN AFRIQUE ONT DES PROBLÈMES. »
>
> – Tariq Khokhar, informaticien

Dans un rapport de 2018, Brookings écrit : « Alors que la cybercriminalité menace les entreprises du monde entier, ce risque est encore plus élevé pour les sociétés africaines ». Bien que l'infrastructure de communication des pays d'Afrique soit comparativement limitée, leur niveau faible de cybersécurité en fait une cible de choix pour les cybercriminels.

La sécurité informatique n'est pas quelque chose de nouveau pour l'Afrique. Dans une étude de 2016, la Business Software Alliance déclare que 57 % des

ENGAGEMENTS NATIONAUX ENVERS LA CYBERSÉCURITÉ



NIVEAU D'ENGAGEMENT :
de **VERT** (le plus haut) à **ROUGE** (le plus bas)

logiciels installés en Afrique et au Moyen-Orient sont piratés, ce qui encourage les attaques cybernétiques et provoque une perte potentielle de 3,7 milliards de dollars. L'informaticien Tariq Khokhar déclare : « Ce n'est pas une exagération de dire que 80 % de tous les ordinateurs qui se trouvent en Afrique ont des problèmes. »

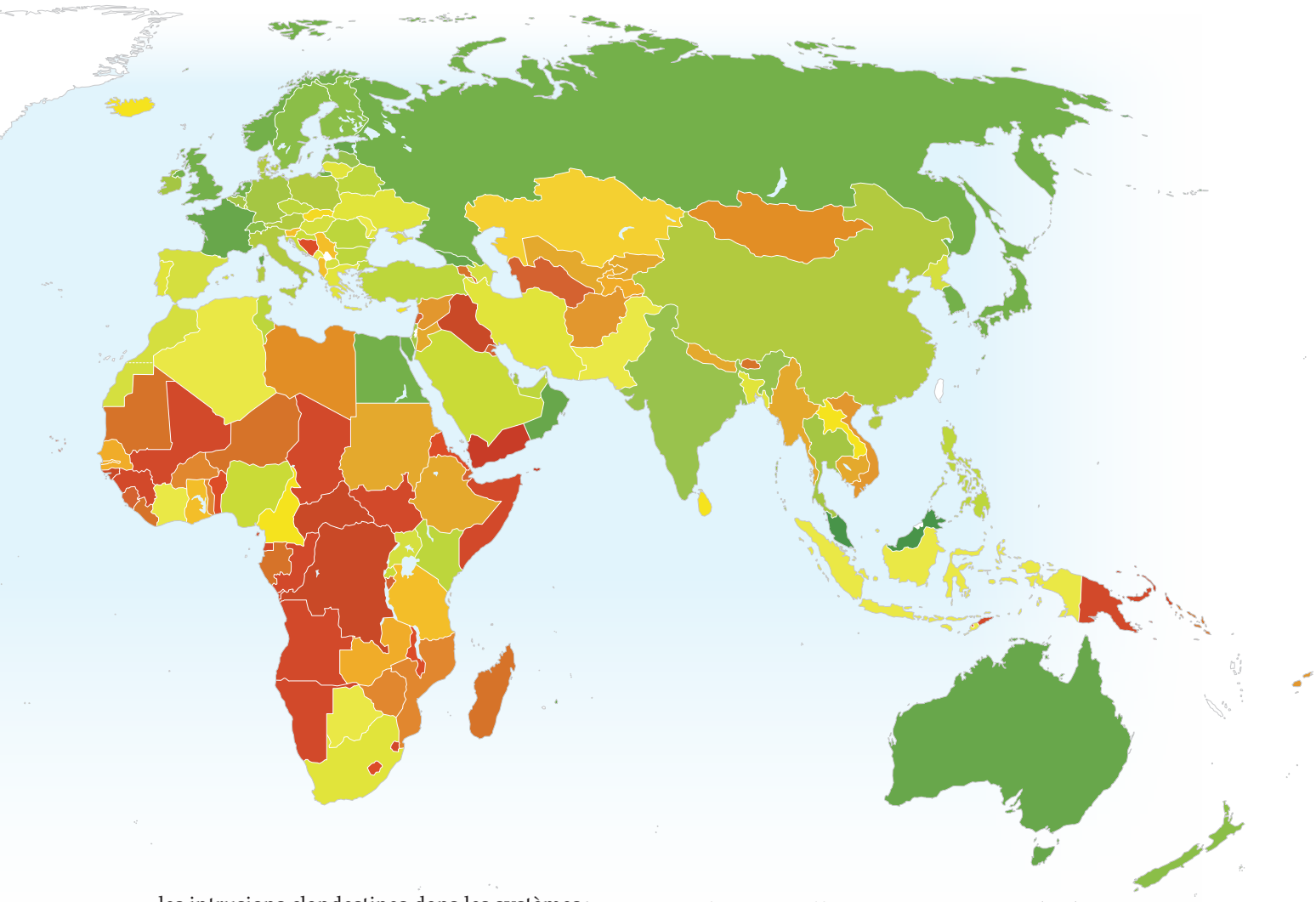
Les pays d'Afrique ne se développeront pas s'ils ne font pas face à la cybersécurité. Le règlement général de l'Union européenne sur la protection des données, décrit par l'UE comme « le changement le plus important depuis 20 ans dans les règlements sur les données à caractère personnel », est en vigueur depuis mai 2018, et les pays africains qui souhaitent maintenir leurs liens commerciaux avec l'Europe devront se conformer à la réglementation européenne.

La cybercriminalité affecte tous les aspects de la vie en Afrique. Le « Rapport de 2017 sur la cybersécurité en Afrique » déclare que les banques et les services financiers africains subissent près d'un quart des pertes du continent causées par le cybercrime, suivis par les gouvernements, l'e-commerce, les transactions sur téléphone portable et les télécommunications.

LES ENJEUX PARTICULIERS DU NIGERIA

Même avant l'arrivée de l'Internet, le Nigeria était tristement connu pour ses fraudes, par exemple celle du « prince nigérian » qui a hérité d'une fortune mais nécessite le numéro de compte bancaire de quelqu'un pour y déposer son argent. De ce fait, le Nigeria a une longueur d'avance pour affronter la cybercriminalité. Dans une étude de 2013 conduite par l'*International Journal of Cognitive Research in Science, Engineering and Education*, des chercheurs présentent les mesures de base que doit prendre un système pour faire face aux cybercrimes :

- Enseigner aux utilisateurs de maintenir continuellement et de mettre à jour leurs systèmes de sécurité informatique. Les entreprises et les organisations doivent aussi être requises d'adopter les meilleures pratiques concernant la gestion informatique efficace.
- Établir des programmes et des forums de technologie de l'information pour les jeunes : cela non seulement armera une nouvelle génération contre le cybercrime, mais offrira aussi de nouveaux emplois à une classe de personnes qui sont sous-employées.
- Utiliser des systèmes de vérification d'adresse pour s'assurer que l'adresse des formulaires de commande de produit correspond à l'adresse de la facture envoyée à l'acheteur.
- Employer des serveurs vocaux interactifs, technologie qui recueille l'« empreinte vocale » ou autorisation et vérification vocale des clients avant d'expédier les commandes.
- Le suivi des adresses IP assure que l'adresse IP liée à la commande d'un client est celle du pays figurant sur les adresses de facturation et d'expédition de la commande.
- Utiliser des systèmes de télésurveillance.
- Les logiciels antivirus et anti-espions préviennent et bloquent les virus informatiques, et ils limitent



Source : Rapport 2017 de l'indice mondial de la cybersécurité

les intrusions clandestines dans les systèmes informatiques.
- Les pare-feu protègent les réseaux informatiques contre les entrées non autorisées.
- La cryptographie chiffre les informations de façon que seuls l'expéditeur et le destinataire présumé puissent les décrypter.
- La « cyberéthique » et la « cyberlégislation » exigent que les fournisseurs d'accès à l'Internet prennent des mesures pour se protéger contre le cybercrime.

LA DÉFENSE CONTRE LA CYBERCRIMINALITÉ

Landry Signé et Kevin Signé écrivent pour la Brookings Institution qu'il existe quatre étapes que les entreprises africaines doivent suivre pour faire face à la cybercriminalité. Bien que ces étapes visent le secteur commercial, elles représentent aussi de bonnes pratiques pour d'autres secteurs.

1. Conception et déploiement de la « cyberrésilience » : Dans son rapport sur l'« État de la cybersécurité en 2018 », ISACA, appelée antérieurement Information Systems Audit and Control Association [Association pour les audits et le contrôle des systèmes d'information], déclare que quatre professionnels de la sécurité sur cinq dans le monde pensent que leur entreprise sera probablement ou très probablement victime d'une attaque cybernétique au cours de l'année. La moitié des participants indiquent que leur organisation a enregistré une augmentation des attaques au cours des douze derniers mois. La prévention ou l'arrêt des attaques cybernétiques commence au niveau exécutif « en priorisant et en adoptant des procédures qui protègeront les actifs de grande valeur et en les intégrant obligatoirement dans tous les processus commerciaux », selon le rapport de Brookings. Les sociétés doivent améliorer leurs mesures de sécurité en :

- développant les aptitudes de leurs employés concernant la sécurité de l'information
- sécurisant leurs systèmes d'information et mettant à jour régulièrement leur infrastructure
- utilisant des technologies de surveillance active
- mettant en œuvre des systèmes de détection proactive et de réponse rapide pour faire face aux violations et aux incidents liés à la sécurité
- effectuant régulièrement des contrôles de sécurité et des tests de pénétration

2. Développement des aptitudes en cybersécurité : Le plus grand problème affectant le continent pourrait être le

DES PAYS AFRICAINS MONTRENT LA VOIE POUR

COMBATTRE LA CYBERCRIMINALITÉ

PERSONNEL D'*ADF*

Pour faire face à la cybercriminalité, les pays d'Afrique sont désavantagés par le manque d'expertise locale et la carence des lois traitant de cette question. Mais il y a des pays qui affrontent directement le problème. Le « Rapport de 2017 sur la cybersécurité en Afrique » publié par la société de cybersécurité Serianu indique que les pays suivants excellent dans leur traitement des cybercrimes :

ÎLE MAURICE

Le petit pays de l'île Maurice, dont la population atteint à peine 1,2 million, est devenu le chef de file de la technologie de l'information et des communications en Afrique.

Les responsables du gouvernement déclarent que le pays préconise une loi commune sur la cybersécurité pour toute l'Afrique. L'île Maurice est l'un des premiers pays africains à avoir changé ses lois sur la confidentialité pour se conformer au règlement général de l'Union européenne sur la protection des données.

Dans son indice mondial de la cybersécurité de 2017, l'Union internationale des télécommunications déclare que le projet de pistage et de détection des botnets de l'île Maurice a permis à l'équipe de réponse aux urgences informatiques du pays de « prendre proactivement des mesures pour réduire les menaces pesant sur différents réseaux du pays ».

« Le développement des capacités est un autre secteur dans lequel l'île Maurice obtient de bons résultats, selon l'indice. L'unité de sécurité TI du gouvernement a conduit 180 sessions de sensibilisation pour quelque 2.000 fonctionnaires dans 32 ministères d'état depuis 20 ans. »

RWANDA

L'indice a classé le Rwanda en deuxième place pour la cybersécurité en Afrique. Comme l'île Maurice, le Rwanda préconise des protocoles de sécurité pour l'ensemble du continent. Les responsables rwandais déclarent que leurs protocoles et leurs lois ont stoppé 8 millions d'attaques cybernétiques en 2017.

L'index indique que le Rwanda « a une politique de cybersécurité indépendante qui concerne le secteur public aussi bien que privé » et qu'il s'est « engagé à développer une industrie de cybersécurité plus forte pour assurer la résilience du cyberespace ».

KENYA

L'index classe le Kenya en troisième place sur le continent, en notant que le Centre national de coordination des équipes de réponse aux incidents informatiques du Kenya coordonne la cybersécurité au niveau national, régional et mondial. Le Kenya, centre africain des transactions sur portable, a adopté en mai 2018 une loi sur l'usage abusif de l'informatique et la cybercriminalité.

Le 19 décembre 2018, l'Autorité des communications du Kenya a déclaré que le nombre d'attaques cybernétiques détectées dans le pays était passé à 3,8 millions entre juillet et septembre 2018, soit une augmentation de 400.000 menaces comparé au trimestre précédent. Début 2019, le centre avertit le public qu'il a détecté « Emotet », maliciel qui cible les systèmes réseaux du monde entier.

NIGERIA

Le Nigeria est en quatrième position en Afrique pour la défense contre la cybercriminalité, malgré sa réputation mondiale concernant les fraudes cybernétiques et autres cybercrimes. IDG, société médiatique de haute technologie, déclare que la cybercriminalité a été « un cauchemar pour l'image du pays ». Même avec ses avancées en matière de sécurité, le Nigeria a perdu 649 millions de dollars en 2017 à cause des activités liées aux cybercrimes, la somme la plus élevée du continent.

Toutefois, le pays a proposé une taxe qui aiderait les agences à lutter contre la cybercriminalité. L'impôt de 0,005 % sur les entreprises de télécommunication a été proposé dans la loi de 2015 sur la cybercriminalité pour former les agents de cybersécurité. Bien qu'il soit le pays le plus peuplé d'Afrique avec près de 200 millions d'habitants, le Nigeria possède seulement 1.800 professionnels homologués en cybersécurité.

manque de spécialistes de la cybersécurité chevronnés et compétents. Les responsables des gouvernements et des entreprises doivent attirer de tels spécialistes ou obtenir les ressources nécessaires à leur formation. Mais il sera difficile de garder ces spécialistes. « Les organisations africaines doivent adopter des stratégies efficaces pour faire face à l'exode des cerveaux affectant les employés de cybersécurité les plus talentueux, écrivent les auteurs. En effet, lorsqu'ils obtiennent les qualifications nécessaires, ces spécialistes deviennent de plus en plus mobiles et peuvent choisir de partir, surtout pour l'Europe ou l'Amérique du Nord. » Actuellement, moins de 1 % des programmes de gestion des aptitudes de sécurité traitent du recrutement expérimental et de la rétention des experts. Selon les auteurs, ce chiffre passera à 20 % en 2020.

3. Protection de l'intégrité des données : La protection des données pourrait remplacer la confidentialité comme but principal de la cybersécurité. De nombreux cas récents de logiciel de rançon, dans lesquels le logiciel prend le contrôle du système ou des données informatiques jusqu'à ce qu'une rançon soit payée, ont souligné l'importance de l'intégrité des données. Aucune des entreprises qui avaient payé une rançon n'a pu confirmer qu'elle avait finalement récupéré toutes ses données. Les entreprises et autres organismes doivent améliorer leurs mesures de sécurité pour prévenir les attaques par logiciel de rançon et la corruption massive des données.

En plus de la sauvegarde fréquente des données, il existe de nouvelles technologies qui enregistrent les transactions sur plusieurs ordinateurs liés par réseau pair-à-pair. Certains pays, notamment en Afrique du Nord, explorent déjà de nouvelles technologies pour affronter les menaces sur la sécurité. La Brookings Institution déclare que les dépenses concernant la sécurité de l'information au Moyen-Orient et en Afrique du Nord ont augmenté de 11 % en 2017, pour atteindre une valeur totale de 1,8 milliard de dollars.

4. Intégration de la sensibilisation au risque cybernétique dans le processus de prise de décision : Les objectifs, les systèmes et l'actif d'une organisation liés à la cybersécurité ne devraient pas concerner uniquement les cadres supérieurs et l'équipe de cybersécurité. Le but consiste à « populariser une culture sensibilisée au risque cybernétique à tous les niveaux ». En outre, les responsables de l'organisation « doivent être davantage conscients de leur responsabilité en cas d'attaque cybernétique, et doivent reconnaître le besoin d'avoir des gestionnaires compétents pour identifier et affronter les menaces cybernétiques potentielles ».

ISACA déclare que seulement 21 % des directeurs mondiaux de la sécurité des systèmes d'information dépendent directement du chef d'entreprise, alors que 63 % dépendent du directeur des systèmes d'information. Cette structure signifie que ces entreprises considèrent que la cybersécurité est une question plus technique que financière, ce qui est une erreur selon ISACA. ❑

CONCURRENTS ET CAMARADES

L'OSMA MONTRE QUE LA COMPÉTITION ATHLÉTIQUE ENTRE LES SOLDATS PEUT AVOIR UN GRAND IMPACT

PERSONNEL D'*ADF* - PHOTOS PAR OSMA

Le cinquième championnat de boxe militaire africain (CAMBOXE) débute en octobre 2018 en Algérie.

L'Organisation du sport militaire en Afrique en Afrique (OSMA) a été créée avec un objectif simple à l'esprit : bâtir des ponts d'amitié grâce aux sports. Les organisateurs pensent que la compétition athlétique entre les soldats de l'ensemble du continent peut accomplir ce que des heures d'exercice, des conférences et d'autres entraînements militaires ne pourraient pas accomplir.

Les concurrents s'affrontent lors de CAMBOXE 2018 à Alger (Algérie).

« Elle contribue à l'effort de paix global en développant les idéaux de fraternité, d'hospitalité, d'intégration et d'entente mutuelle qui caractérisent les forces armées africaines », déclare le colonel David Kadré du Burkina Faso, président de l'OSMA, à journaldebrazza.com. « Ces idéaux sont chers à nos dirigeants africains pour le développement économique et l'émergence de notre cher continent. »

Fondée en 1994, l'OSMA est la branche régionale africaine du Conseil international du sport militaire, organisation fondée il y a 71 ans et basée à Bruxelles. Le siège social de l'OSMA est situé à Yaoundé (Cameroun) et elle organise des tournois annuels de boxe, de basket-ball, de football et autres sports. Elle compte 45 pays membres.

Les concurrents déclarent que les avantages de la compétition athlétique peuvent être constatés très loin des centres de sport. Des études sur les athlètes militaires ont montré qu'elle peut aider les soldats à éviter les blessures ailleurs que sur les champs de bataille et à se rétablir des traumatismes psychologiques causés par la guerre.

En octobre 2018, environ 100 boxeurs de 14 pays se sont rencontrés à Alger (Algérie) pour le cinquième championnat de boxe militaire africain (CAMBOXE). Pendant cinq jours de compétition acharnée, les participants ont non seulement boxés mais aussi discutés des questions d'intérêt mutuel et se sont réunis lors d'événements sociaux et de festivités. Les athlètes algériens ont gagné le plus de médailles, suivis par ceux du Kenya et de la Tunisie.

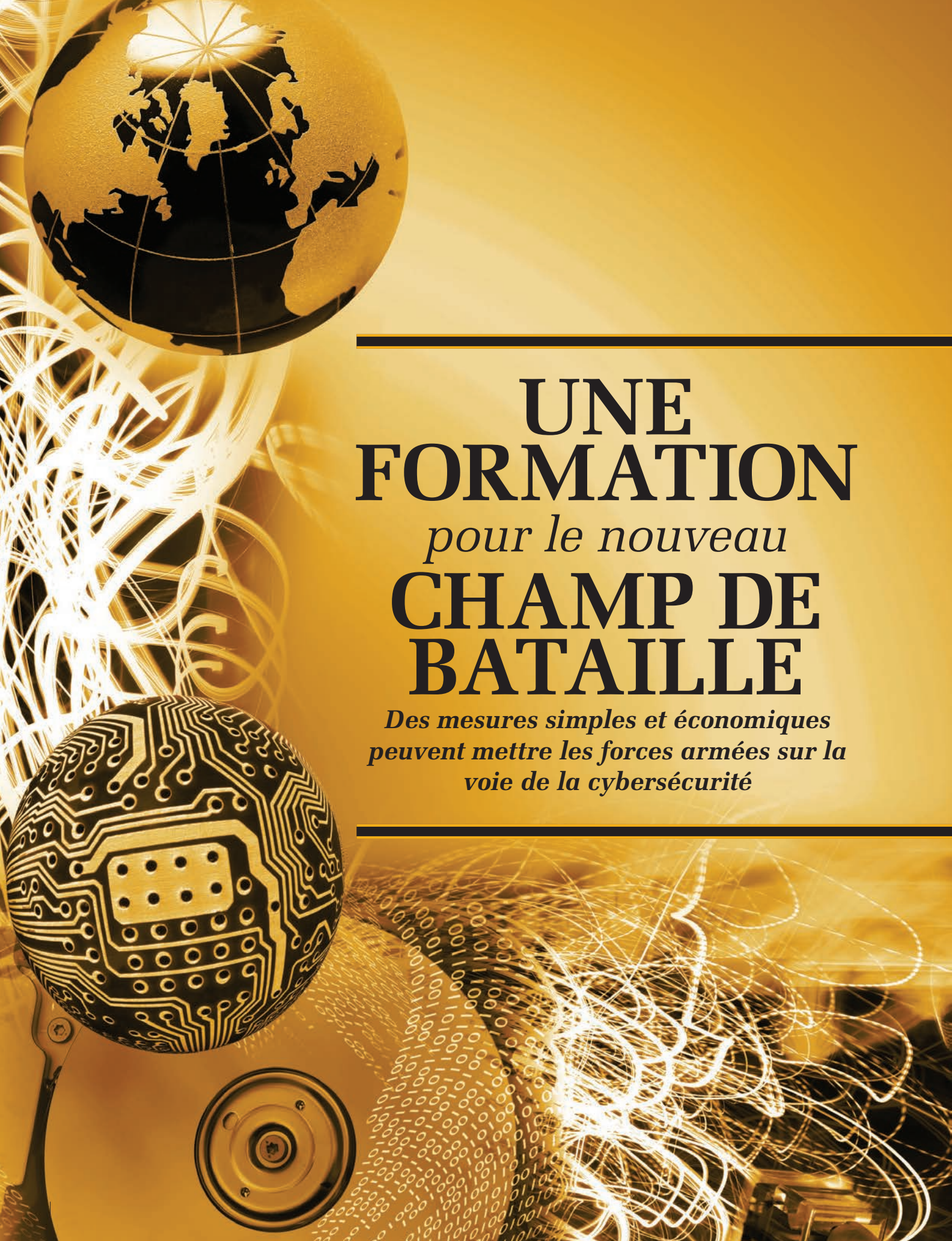
En 2018 aussi, des athlètes de l'OSMA ont participé à une course de cross à Luanda (Angola) et à un championnat de basket-ball à Brazzaville (République du Congo), dans lequel le Congo a remporté la première place, devant le Maroc et l'Angola.

Le colonel Kadré déclare que les événements, auxquels assistent les supporteurs provenant de toutes les classes sociales, offrent une excellente opportunité de promouvoir les relations entre civils et militaires. Il pense qu'ils aident à humaniser les soldats.

« Un tableau d'amitié entre le peuple et l'armée, c'est de cela qu'une nation a besoin, déclare-t-il. C'est seulement lorsque le peuple et l'armée sont unis que nous pouvons dire que la relation est équilibrée. »

Le colonel Kadré espère aussi qu'une organisation telle que l'OSMA pourra réparer l'image des forces armées africaines, qui a été trop souvent souillée par l'indiscipline et les accusations de violence contre les civils. « Les histoires de guerre et de destruction éclipsent en général les bonnes nouvelles. Mais le sport est quelque chose qui peut conduire à des changements », déclare-t-il.

« J'espère que les pays africains utiliseront le sport comme moyen d'éviter les disputes et permettront des changements positifs de développement et d'amitié, déclare le colonel Kadré. Cela est précisément l'un des objectifs principaux de l'OSMA, et c'est aussi quelque chose pour laquelle l'organisation fait de grands efforts au niveau du continent. » ❑



UNE FORMATION *pour le nouveau* CHAMP DE BATAILLE

Des mesures simples et économiques peuvent mettre les forces armées sur la voie de la cybersécurité

PERSONNEL D'*ADF*

Un employé qui passait l'une de ses innombrables journées devant un écran d'ordinateur a ouvert un e-mail et a cliqué sur un lien. Et l'invasion commença.

Cet employé était un technicien informatique de Saudi Aramco, grande société de pétrole d'Arabie saoudite. Il était censé avoir suivi une bonne formation sur l'utilisation prudente des ordinateurs. Mais ce ne fut pas le cas le 15 août 2012, pendant le mois sacré du Ramadan. Un clic sur ce lien était tout ce dont avaient besoin les hackers, qui se faisaient appeler le « Glaive tranchant de la justice », pour infiltrer l'une des sociétés les plus riches du monde.

En quelques heures seulement, 35.000 ordinateurs de la société furent détruits ou partiellement oblitérés, selon un rapport de CNN. Les écrans commencèrent à clignoter. Les ordinateurs s'arrêtèrent.

Les fichiers disparurent. Les employés de la société dans le monde entier tentèrent de se déconnecter des serveurs et de l'Internet en espérant stopper la marche destructrice du virus.

Saudi Aramco continua à produire ses 9,5 millions de barils par jour ; les forages et l'extraction se poursuivirent. Mais l'attaque plongea les fonctions administratives telles que la gestion logistique, l'expédition et les questions contractuelles dans l'âge de pierre du papier et des machines à écrire.

Il n'y avait pas d'Internet, pas de service d'e-mail de la société. Même les téléphones étaient silencieux. Si un contrat devait être signé, les employés l'envoyaient par télécopieur, une page après l'autre. La société a même dû refuser l'accès aux camions-citernes qui cherchaient à se ravitailler. Après plus de deux semaines de paralysie, Saudi Aramco a fait cadeau de son pétrole pour maintenir sa production nationale.

Immédiatement après l'attaque, la société acheta simultanément 50.000 nouveaux disques durs d'ordinateur, en payant plus que le prix du marché pour avoir priorité. Cet achat étrangla l'approvisionnement mondial en disques durs.

« Tous ceux qui ont acheté un ordinateur ou un disque dur entre septembre 2012 et janvier 2013 ont dû payer un prix un peu plus élevé », déclare à CNN Chris Kubecka, ex-conseiller de sécurité de Saudi Aramco.

Un seul e-mail. Un seul lien. Un seul clic. Cela suffit pour perdre un combat dans le cyberespace. Aucun pays n'est immunisé. Aucune armée ne peut être trop préparée.

La Chine, la Corée du Nord et la Russie ont déjà montré leur désir et leur capacité d'attaquer les autres pays dans le domaine cybernétique, en prenant pour cible les élections et l'infrastructure, entre autres. Bien qu'un grand nombre de pays africains ne semblent pas offrir de cible importante, ils ne peuvent pas s'abandonner à l'autosatisfaction, déclare le Dr Jabu Mtsweni, chef d'un groupe de recherche sur la guerre cybernétique au Conseil pour la recherche scientifique et industrielle d'Afrique du Sud. « Les menaces sont fortes, déclare le Dr Mtsweni, et je ne pense pas que nous soyons immunisés contre l'une quelconque d'entre elles. »

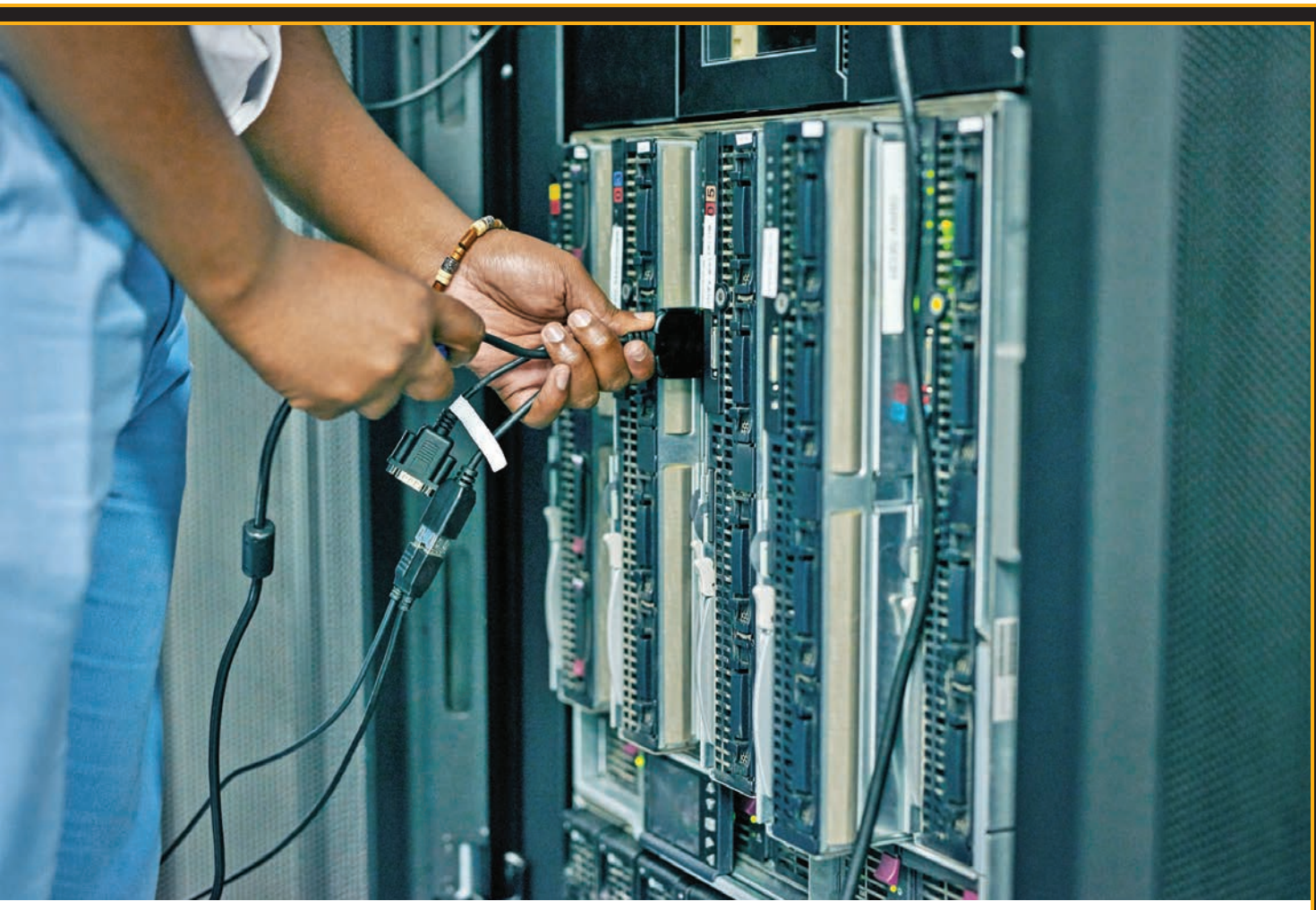
LA SOLUTION COMMENCE PAR LA FORMATION

L'établissement d'une formation solide et l'enseignement des meilleures pratiques offrent la meilleure façon d'assurer que les forces armées africaines soient prêtes à affronter les menaces cybernétiques. Les experts conviennent que tout le monde peut prendre des mesures pour réduire les risques d'un grand éventail de menaces cybernétiques, même si des spécialistes ou un matériel de haute technologie ne sont pas disponibles. Les pays peuvent fournir cette formation aux soldats et aux officiers dans des établissements pédagogiques militaires professionnels.

De telles académies de formation militaire existent dans l'ensemble du continent et beaucoup d'entre

CAPITAINE DE CORVETTE DESIREE FRAME/ÉTAT-MAJOR UNIFIÉ DES ÉTATS-UNIS POUR L'AFRIQUE

Des participants conduisent un exercice de simulation en cybersécurité pendant Africa Endeavor au Cap-Vert, en août 2018.



elles se concentrent sur toute une gamme de sujets, notamment le maintien de la paix et les stratégies de guerre. La cybersécurité n'a pas encore atteint la popularité des autres enseignements militaires plus traditionnels. Cela est dans une large mesure dû à un manque de sensibilisation, déclare le Dr Mtsweni, et à un manque de personnel possédant une formation, une expérience et un intérêt dans les questions de cybersécurité. La plupart des forces armées africaines, déclare-t-il, continuent à se concentrer sur les tactiques et les stratégies de guerre traditionnelles et cinétiques. La modification de cet état d'esprit nécessitera des changements, et du temps.

« Je pense que la première étape devrait commencer principalement au niveau du recrutement », déclare le Dr Mtsweni à *ADF*. « Autrement dit, lorsque l'armée recrute, elle doit commencer à recruter pour l'ère du numérique. »

C'est plus facile à dire qu'à faire. Où que ce soit, les gens qui possèdent des aptitudes en cybersécurité sont peu nombreux. Un certain degré d'intérêt et d'aptitude est essentiel, parce que l'intérêt et le talent technologiques ne sont pas à la portée de tous. Même la mise en place et la fourniture de la formation sont insuffisantes. Il doit exister une opportunité d'utiliser et de développer les nouvelles aptitudes. Les officiers et les soldats qui ont reçu une formation cybernétique deviendront découragés s'ils n'ont pas de moyen de pratiquer leur formation. Le Dr Mtsweni déclare que ceux qui sont formés devront être capables de mettre en œuvre ce qu'ils ont appris.

TROUVER UN CHAMPION

Le Dr Greg Conti, stratégiste en sécurité pour IronNet Cybersecurity aux États-Unis, a dirigé le Centre de recherche cybernétique de l'Académie militaire des États-Unis à West Point et son Institut cybernétique de l'Armée de terre. Il déclare à *ADF* que la meilleure façon de lancer une formation efficace en cybersécurité est d'avoir « un cadre supérieur champion ». L'alternative consisterait à attendre que le changement se produise à partir de la base. Cela serait plus lent, et moins probable au sein d'une hiérarchie militaire.

Le Dr Mtsweni convient qu'il est crucial de trouver un champion. « Tous les succès et les échecs dépendent du leadership. S'il existe donc un chef qui

À mesure que l'utilisation des ordinateurs et autres dispositifs électroniques continue à augmenter en Afrique, les gouvernements et les forces armées devront renforcer les mesures liées à la cybersécurité.

est le champion de la cybersécurité, vous découvrez que les forces sur le terrain peuvent le suivre plus facilement, déclare le Dr Mtsweni. Dans un contexte africain, cela est plus rare car la plupart des colonels et des généraux ont été formés à la vieille école. En Afrique du Sud, nous disons qu'ils sont nés "BT" (avant la technologie). On les appelle des BT : ils sont nés avant la technologie en ce sens qu'il leur est très difficile de comprendre ce que vous dites lorsque vous parlez de la cybersécurité, parce qu'ils ne l'ont pas apprise dans leur formation militaire. Ils n'ont jamais été vraiment introduits à la cybersécurité. »

Si un haut dirigeant s'intéresse à la cybersécurité, ceux qui ont un grade inférieur le suivront. Il n'est même pas nécessaire que le dirigeant ait une compétence technique ou de bonnes connaissances du sujet, mais seulement qu'il réalise son importance et qu'il s'engage à y faire face avec de l'argent, des ressources, un espace et une attention continue. Ceci, déclare le Dr Conti, aidera les autres à comprendre l'importance de la cybersécurité et à s'y investir. La priorité du haut dirigeant se propagera vers le bas de la structure du commandement.

Ensuite, le dirigeant devra identifier, conserver et promouvoir le personnel possédant le talent et

les aptitudes nécessaires. Si une unité peut identifier et responsabiliser un spécialiste en cybersécurité et l'aider à croître, les résultats « changeront la donne », déclare le Dr Conti.

Une fois que le personnel est identifié, il existe des options de formation qui peuvent fournir des résultats tangibles sans nécessiter de dépenses énormes. Par exemple, il existe tout un éventail d'informations gratuites en ligne sur la cybersécurité. Le personnel pourrait aussi travailler à partir de livres qui coûtent environ 30 dollars.

Si davantage d'argent est disponible, le Dr Conti déclare qu'une force militaire pourrait envoyer quelqu'un pour suivre une formation, lequel reviendrait ensuite pour donner des briefings à ses collègues et partager sa documentation. Une telle personne pourrait devenir l'« expert local » en cybersécurité, à un coût non récurrent de plusieurs milliers de dollars pour les frais de voyage et de scolarité.

UNE FORMATION EFFICACE À BAS PRIX

Les connaissances en cybersécurité et les bonnes habitudes sécuritaires peuvent être efficaces sans coûter trop cher. La formation peut être personnalisée pour les soldats et les officiers, selon leur expérience et leurs responsabilités. Le Dr Conti déclare qu'il est crucial de fournir une dose appropriée de formation en cybersécurité aux personnes appropriées et au moment approprié de leur carrière. Les besoins d'un simple soldat sont probablement différents de ceux d'un sous-officier ou d'un officier.

Il déclare que la formation peut être ciblée pour un groupe important, pour quelques-uns ou pour peu de personnes. La formation la plus importante destinée au plus grand nombre traiterait de l'« hygiène cybernétique ». Cela concerne toutes les mesures fondamentales que tout le monde doit prendre dans le cyberespace. Sans elles, tout le reste échoue.

Elles incluent notamment le maintien du caractère privé des mots de passe, le changement fréquent des mots de passe et le refus de cliquer sur des liens ou des pièces jointes ouvertes dans les e-mails non sollicités ou suspects. Le simple fait de prendre un selfie avec un téléphone portable pendant une opération et de l'afficher sur les sites des réseaux sociaux peut compromettre une mission sensible.

Il est aussi important de s'assurer que les ordinateurs militaires exécutent des versions propres des logiciels populaires. Le Dr Conti raconte que les bazars d'Irak vendaient Microsoft Office pour 1 à 3 dollars. Il déclare que, sans aucun doute, ces logiciels étaient pleins de virus, de maliciels et autres codes malveillants.

La formation suivante est destinée à ce que le Dr Conti appelle le groupe des « quelques-uns ». Il inclut les intervenants qui travaillent de temps à autre en cybernétique, par exemple les avocats et les responsables politiques, les planificateurs militaires et ceux qui construisent et exploitent les réseaux informatiques. Une formation sur les 20 principaux contrôles de base du Centre pour la sécurité de l'Internet (CIS) serait utile pour ce groupe, selon le Dr Conti. Leur liste inclut l'inventaire et le contrôle du matériel et des logiciels, les protections des e-mails et des navigateurs Internet, les défenses contre les maliciels, le contrôle de l'accès sans fil, la surveillance des comptes, la réponse aux incidents et les tests de pénétration, entre autres.

La liste du CIS représente « l'ensemble canonique des meilleures pratiques [de l'industrie] pour sécuriser votre infrastructure TI », déclare le Dr Conti, en ajoutant que cette liste peut probablement protéger contre 80 % des menaces de niveau faible ou moyen. Les personnes qui appartiennent au groupes des « quelques-uns » pourraient aussi obtenir des certifications additionnelles telles que celle de Professionnel homologué de la sécurité des systèmes d'information.

La catégorie des « peu nombreux » inclut ce que le Dr Conti appelle les « vrais spécialistes de la cybersécurité », tels que les opérateurs pratiques sur clavier qui gèrent les capacités cybernétiques offensives et défensives. Leur formation serait hautement spécialisée et inclurait probablement une expertise dans le renseignement d'origine électromagnétique et la façon de l'utiliser pour les opérations de guerre cybernétique, dans la politique et le droit cybernétiques, dans l'analyse du renseignement, dans la gestion des réseaux informatiques et dans la façon d'intégrer la cybernétique avec les opérations cinétiques et vice-versa.

LA CROISSANCE DE LA SENSIBILISATION

Le Dr Mtsweni déclare que plusieurs pays africains commencent à démontrer une sensibilisation croissante concernant l'importance de la cybersécurité. Il déclare que les pays tels que le Ghana, le Kenya, l'île Maurice, le Rwanda, le Sénégal et l'Afrique du Sud montrent un engagement envers la cybersécurité. Les forces armées suivent en général les gouvernements : à mesure que les gouvernements continuent à prioriser la cybersécurité, il est probable que les forces armées nationales suivront.

Toutefois, le développement des capacités nationales en cybersécurité prendra du temps, peut-être cinq ans ou plus, selon le Dr Mtsweni.

Le Dr Conti déclare qu'il en sera ainsi quel que soit le niveau de formation du personnel militaire. L'attention à la cybersécurité ne peut pas être passagère. « Elle doit faire partie d'une vision à long terme. » ❑

ILLUSTRATION D'ADF

La réfutation du MESSAGE

POUR BLOQUER LA PROPAGANDE EXTRÉMISTE EN LIGNE, IL NE SUFFIT PAS DE STOPPER LE MESSAGER

PERSONNEL D'*ADF*

Pendant des années, le plan suivi pour réfuter la propagande extrémiste était simple : répéter aux adeptes que leurs croyances étaient erronées et qu'ils en souffraient. Leur dire d'abandonner leur cause, car leur vie s'améliorerait s'ils changeaient leurs idéaux. Répéter les messages de réfutation aussi souvent que nécessaire.

Mais les contre-messages ont un problème : ils fonctionnent rarement.

Le Dr Cristina Archetti, auteur de « Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age » [Le terrorisme, les communications et les nouveaux médias : expliquer la radicalisation dans l'ère du numérique], déclare que les développeurs de messagerie anti-extrémiste doivent abandonner les anciens modèles.

« Pour commencer, depuis les rapports sur la façon de contrecarrer la radicalisation en ligne jusqu'aux appels des gouvernements visant à éliminer les sites extrémistes de l'Internet, on se concentre fortement sur les messages, écrit le Dr Archetti. Que cette approche se traduise par la lutte contre les terroristes avec un contre-message correct ou par l'élimination de leurs messages extrémistes, elle reflète un modèle tout à fait obsolète des interactions avec les médias publics. »

Le Dr Archetti déclare qu'un tel modèle, parfois appelé communication de type « aiguille hypodermique », a été développé après la Première Guerre mondiale lorsque les vainqueurs ont pensé qu'ils avaient gagné au moins en partie à cause de leurs pouvoirs persuasifs de propagande.

Un tel modèle est aujourd'hui largement reconnu comme étant simpliste et naïf. Comme le remarque le Dr Archetti, « nous pouvons tous nous rendre compte dans l'immédiateté de notre vie quotidienne que nous n'achetons pas tous les produits que les messages publicitaires nous disent d'acheter ».

Aujourd'hui, les extrémistes utilisent l'Internet et les réseaux sociaux pour recruter des adeptes, en général de jeunes ados ou des personnes d'une vingtaine d'années. Les extrémistes utilisent des vidéos de haute qualité pour convaincre ces jeunes qu'ils sont victimes de discrimination à cause de leurs croyances.

« L'EIIL utilise à bon escient YouTube, Twitter, Instagram, Tumblr, les mèmes de l'Internet et autres réseaux sociaux », signale *The Guardian* du Royaume-Uni. « Les vidéos et les photos d'amateur sont aussi téléchargées quotidiennement par ses fantassins ; elles sont ensuite disséminées mondialement, par les utilisateurs ordinaires et par les grands organismes de presse

qui recherchent les images d'un conflit auquel leurs propres caméras ne peuvent pas accéder. »

Cet auditoire cible est situé dans les régions du monde où les jeunes ont peu de chance de trouver un emploi, et où l'insatisfaction concernant le gouvernement et le statu quo est élevée. Les gouvernements et les spécialistes de la technologie de l'information se sont jetés dans la mêlée et s'efforcent de stopper les messages des extrémistes tout en essayant de développer des contre-messages.

« Il est crucial de mettre à profit les contributions potentielles de toutes les parties prenantes, notamment les entreprises Internet et les utilisateurs Internet. »

— « Contrecarrer la radicalisation en ligne : une stratégie d'action », M. Tim Stevens et Dr Peter R. Neumann

Mais cela s'avère compliqué. Les messages doivent être exprimés de façon que l'auditoire cible les considère comme sympathiques et amicaux. Les contre-messages doivent avoir un côté personnel et souligner que la doctrine des extrémistes est basée sur des mensonges et des distorsions.

LES APPROCHES INSTINCTIVES

Les chercheurs déclarent que les premières approches instinctives pour contrecarrer les messages des extrémistes sur l'Internet se sont concentrées sur des solutions techniques, en supposant que l'élimination ou le blocage de ces messages résoudrait le problème. Dans une étude de 2009 intitulée « Contrecarrer la radicalisation en ligne : une stratégie d'action », les chercheurs Tim Stevens et Peter R. Neumann ont déclaré qu'une telle approche technique était « nécessairement rudimentaire, onéreuse et contre-productive ».

M. Stevens et le Dr Neumann déclarent que toute stratégie visant à réfuter la radicalisation en ligne doit créer un environnement dans lequel la création et la visualisation de ces messages deviennent non seulement plus difficiles d'un point de vue technique, mais aussi inacceptables et peu souhaitables. Ils notent que les gouvernements à eux seuls ne peuvent pas stopper les messages extrémistes en ligne. « Il est crucial de mettre à profit les contributions potentielles de toutes les parties prenantes, notamment les entreprises Internet et les utilisateurs Internet. » Ils recommandent aussi les points suivants :

- **Dissuader les producteurs :** L'utilisation sélective du démantèlement des sites Internet et des réseaux sociaux, accompagnée de poursuites intentées contre les producteurs responsables, « signalerait que les personnes engagées dans l'extrémisme en ligne ne sont pas au-dessus de la loi ».
- **Responsabiliser les communautés en ligne :** La création d'un « panel d'utilisateurs Internet » pour améliorer les mécanismes de rapport et les procédures de plainte permettrait aux utilisateurs de contribuer à la stratégie anti-extrémiste.
- **Réduire l'attrait du message :** « Il faut faire davantage attention à l'éducation aux médias et une approche exhaustive dans ce domaine est absolument nécessaire », écrivent les auteurs.
- **Promouvoir des messages positifs :** Établir un fonds indépendant de démarrage pour fournir de l'argent aux « projets communautaires en ligne » visant à contrer l'extrémisme. « Il s'agit de tirer parti de l'enthousiasme et de la bonne volonté des communautés du pays qui souhaiteraient investir du temps et des ressources mais qui ont besoin d'un soutien financier limité pour exposer leurs idées sur l'Internet. »

D'autres experts recommandent aussi d'offrir de l'argent aux projets communautaires en ligne. Dans « La tendance du djihad : une analyse exhaustive de l'extrémisme en ligne et de la façon de le contrer », M. Ghaffar Hussain et le Dr Erin Marie Saltman préconisent la création d'un organisme central qui offrira un financement de démarrage et une formation de lutte contre l'extrémisme en ligne au niveau communautaire.

Ces auteurs déclarent : « La lutte contre l'extrémisme en ligne devrait être un effort conjoint entre les parties prenantes du secteur public, du secteur privé et du secteur tertiaire ». Ils suggèrent aussi ce qui suit :

- **Établir un forum** qui traite de l'extrémisme en ligne et qui réunit les parties prenantes des secteurs clés.
- **Améliorer la maîtrise du numérique** et les aptitudes critiques de son utilisation dans les écoles et les communautés.
- **Encourager la création** d'un organe des réseaux sociaux qui clarifie les politiques gouvernementales et réfute la propagande.
- **Conduire un exercice cartographique** pour explorer les efforts actuels visant à affronter l'extrémisme en ligne et pour identifier des partenaires que l'on pourrait aider pour développer une présence efficace en ligne.
- **Effectuer des recherches plus approfondies** sur la façon dont les extrémistes utilisent l'Internet pour diffuser leur propagande.

Cette jeune fille a échappé au groupe extrémiste Boko Haram du Nigeria, lequel est actif dans une région où un grand nombre d'habitants ont été déçus par le gouvernement national. REUTERS

Un homme répare un ordinateur à Khartoum (Soudan). Certains groupes extrémistes sont experts dans la technologie des messageries, aussi est-t-il difficile de les combattre alors que l'Afrique développe ses capacités de connexion en ligne. REUTERS

LA RECONNAISSANCE DES DOLÉANCES

Toutes les stratégies de lutte contre les messages des extrémistes ont un point en commun : le fait qu'aucune contre-mesure passe-partout ne fonctionne dans tous les cas.

Dans son rapport intitulé « La déradicalisation en ligne ? Réfutation des narratifs de l'extrémisme violent : la stratégie des messages, des messagers et des médias », le politologue Omar Ashour déclare qu'il est crucial de « traiter de toutes les dimensions, ainsi que de personnaliser le message pour des auditoires différents, en particulier pour les jeunes et leurs inquiétudes ».

Les extrémistes comprennent depuis des années que le ciblage des auditoires de jeunes par le biais de longs sermons sur l'Internet ne fonctionne pas. Ils ont plutôt adopté une propagande moderne : des vidéos Internet et de brefs messages affichés sur les réseaux sociaux. Et ils ont bien appris à le faire.

Un récit de riposte personnalisé doit éviter la simplification à outrance, la superficialité et les généralisations, car de tels raccourcis invitent ce que M. Ashour appelle des « attaques en retour ». Les contre-messages devraient être attrayants et encourageants, tout en reconnaissant aussi la validité de quelques-unes des doléances, ou même de toutes, par exemple le manque d'emplois et d'opportunités économiques. Le contre-message doit offrir des façons alternatives de régler les doléances tout en mettant l'accent sur « la légitimité et l'efficacité des stratégies basées sur la non-violence ».

Même si ces approches ne sont pas nouvelles, « l'identité des messagers fait une grande différence », déclare M. Ashour. Il mentionne l'exemple d'un groupe islamique qui accepta des récits de riposte après les avoir rejetés précédemment parce qu'ils furent finalement présentés par des gens qu'ils connaissaient et en qui ils avaient confiance.

Après la création des contre-messages et la coordination avec les messagers choisis, il s'agit ensuite de publier et de promouvoir les messages et les messagers sur les médias. M. Ashour remarque qu'« un grand nombre de combats remportés par les extrémistes violents ont eu lieu au niveau des médias ». La dimension médiatique du récit de riposte nécessite trois étapes :

- Analyser les récits de riposte disponibles et souligner leurs points forts et leur pertinence pour l'auditoire ciblé. Évaluer l'impact potentiel.
- Si nécessaire, traduire le message. Puis, le résumer et le simplifier au besoin pour l'adapter à la nature stylisée de certaines plateformes médiatiques. Utiliser des textes et un contenu multimédia, tel que des clips en ligne et des fichiers sonores.
- Présenter les messagers, leurs antécédents et leurs expériences.

NE PAS PRENDRE DE RACCOURCI

La réfutation de la propagande en ligne n'est pas une tâche simple effectuée sur des médias de masse. Un rapport du département d'État des États-Unis

intitulé « Contrer les discours extrémistes en ligne » présente six suggestions pour confronter les recruteurs extrémistes :

- **Ne pas prendre de raccourci :** Bien qu'une stratégie visant à contrer les récits extrémistes en ligne puisse être utile, l'engagement au niveau communautaire reste la pierre angulaire de la diffusion des messages. Il faut contrer la présence des recruteurs dans les communautés.
- **Utiliser un grand éventail de contre-messages :** Ils doivent être associés à des solutions techniques, y compris la clôture des sites Internet et le filtrage du contenu. La clôture des sites est, au mieux, une mesure souvent temporaire parce que les extrémistes lanceront tout simplement de nouveaux sites. Les mesures techniques ont une raison d'être, mais elles doivent être utilisées chirurgicalement pour soutenir un plus grand éventail de mesures de prévention et de lutte contre l'extrémisme violent.
- **Personnaliser le message en fonction de l'auditoire :** Des contre-mesures qui peuvent sembler convaincantes et raisonnables pour des personnes modérées peuvent avoir un effet inverse si elles sont utilisées avec un auditoire qui est plus politisé. Les gens responsables pour créer des contre-messages doivent bien comprendre le point de vue des auditoires qui sont devenus au moins partiellement radicalisés.
- **Fournir des alternatives logiques et honnêtes aux récits extrémistes :** Des recherches indiquent que les gens écouteront les récits et y croiront plus facilement si ceux-ci fournissent des alternatives honnêtes à leurs croyances. Lorsque les extrémistes diffusent des récits mensongers, en affirmant par exemple que les États-Unis prennent pour cible les civils en Irak et en Syrie, il n'est pas suffisant de nier cette allégation. Il faut fournir un contre-message précis.
- **Le messager est important :** Même les populations modérées qui rejettent la majeure partie d'une idéologie extrémiste rejetteront aussi les contre-messages provenant de sources auxquelles elles ne font pas confiance. Les contre-messages doivent provenir de personnes au sein de leur communauté. Ces intervenants doivent être influents et respectés, qualités qui nécessitent souvent du temps pour se manifester.
- **Contrer les croyances incorrectes en présentant des informations correctes :** Le simple rejet des allégations des extrémistes pourrait avoir l'effet contraire de les renforcer. Les contre-messages doivent présenter des affirmations et des faits précis, au-delà d'une simple réfutation.

CHERCHER LES RAISONS

Dans le magazine *The Atlantic*, le rédacteur Graeme Wood déclare que les occidentaux qui accusent les Musulmans de suivre aveuglément d'« anciennes écritures » ne comprennent pas du tout les causes fondamentales de l'extrémisme. Il déclare que les vrais érudits savent mieux ce qu'il en est.

« Ces érudits vous implorent de considérer les conditions dans lesquelles ces idéologies se sont développées : la mauvaise gouvernance, le changement des coutumes sociales, l'humiliation de vivre sur une terre dont la valeur dépend seulement de son pétrole », écrit M. Wood.

Une autre stratégie, déclare M. Ashour, consiste à identifier des événements historiques spécifiques pour donner une légitimité à la dimension politique. Le récit se focalise sur « la glorification des actes violents, notamment le terrorisme, ainsi que celle de leurs auteurs ». Exemple : les vidéos particulièrement violentes que certains extrémistes ont placées sur l'Internet, et qui incluent la torture et la décapitation.

Ce récit met l'accent sur ce qu'il appelle des actions ou des réactions religieusement légitimes à des doléances politiques et à l'oppression sociale. En ce qui concerne al-Qaïda, le groupe souligne que ces actions constituent un devoir religieux personnel.

DÉCOUVRIR CE QUI FONCTIONNE

Quelle que soit l'approche utilisée pour contrer les messages des extrémistes, les résultats doivent être étroitement surveillés. Par exemple, l'argent fourni aux initiatives communautaires est gaspillé si on ne détermine par leur efficacité.

« Il est certain qu'un grand nombre de projets qui pourraient obtenir un soutien vont échouer », écrivent le Dr Neumann et M. Stevens. « Ceci n'est pas surprenant. Après tout, l'Internet est un environnement extrêmement dynamique et les raisons pour lesquelles certains sites échouent alors que d'autres ont du succès ne sont pas claires du tout. Même s'il était possible de trouver une explication, les nouvelles technologies et les nouveaux modes d'interaction pourraient rapidement la rendre inutile. »

Les deux auteurs ajoutent qu'ils ont constaté « un intérêt et une bonne volonté extraordinaires » lorsqu'ils ont conduit leurs recherches. « L'industrie de l'Internet peut par exemple s'inquiéter d'une réglementation gouvernementale autoritaire, mais elle semble être tout à fait prête à contribuer positivement lorsque cela est possible et constructif. De telles expressions d'intention devraient être activement utilisées pour élaborer une stratégie vraiment exhaustive. »

Ils notent que les messagers anti-extrémistes doivent être ouverts aux évolutions de la technologie et des modes d'interaction.

« Par exemple, on pense souvent que l'accroissement du contenu produit par les utilisateurs représente un danger parce qu'une grande partie du contenu associé à la radicalisation en ligne est mis à disposition de cette façon », écrivent-ils. Ils ajoutent que « le contenu produit par les utilisateurs est non seulement un acquis, mais s'il est compris correctement il peut devenir une force puissante contre la radicalisation. » ❑

AFP/GETTY IMAGES

LA « JOCONDE NIGÉRIANE » RETOURNE CHEZ ELLE

REUTERS

La « Joconde nigériane », peinture perdue pendant plus de 40 ans et retrouvée dans un appartement londonien en 2018, a été exposée au Nigeria pour la première fois depuis sa disparition.

Tutu, peinture de Ben Enwonwu, l'artiste nigérian moderne le plus célèbre, a été créée en 1974. Elle a été présentée à l'exposition d'art de Lagos l'année suivante mais ensuite on ignorait où elle se trouvait jusqu'à ce qu'elle réapparaisse dans le Nord de Londres.

Ses propriétaires, qui souhaitaient rester anonymes, se sont adressés à un expert en art africain moderne et contemporain pour identifier la peinture. Il a reconnu le portrait de M. Enwonwu.

Les propriétaires ont mis en vente le portrait et ce dernier a été vendu pour 1,57 million de dollars à un acheteur anonyme lors d'une vente aux enchères. Cette vente en a fait l'œuvre d'art moderne nigérian la plus chère achetée dans une vente aux enchères.

Elle a été prêtée pour être exposée à la foire Art X Lagos au Nigeria.

Tutu est appelée la « Joconde nigériane » du fait de sa disparition et de sa réémergence. Il s'agit de la première œuvre d'un artiste nigérian moderne qui soit vendue pour plus de 1 million de dollars. La *Joconde* originale, portrait exécuté par Léonard de Vinci, avait été volée au Louvre en 1911. Le voleur, Vincenzo Peruggia, l'avait finalement emmenée en Italie où elle avait été récupérée et ramenée au Louvre en 1914.

La peinture nigériane est un portrait d'Adetutu Ademiluyi, petite-fille d'un chef traditionnel du groupe ethnique des Yorubas. Ce portrait a une signification spéciale au Nigeria comme symbole de la réconciliation nationale après la guerre du Biafra de 1967 à 1970.

M. Enwonwu faisait partie du groupe ethnique des Igbos, le groupe le plus important de la région Sud-Est du Nigeria qui avait essayé de se séparer sous le nom du Biafra. Les Yorubas, dont la région d'origine est au Sud-Ouest, soutenaient principalement le parti opposé.

M. Enwonwu a peint trois versions du portrait. Les reproductions, qui ont commencé à être créées dans les années soixante-dix, sont en circulation depuis lors et un grand nombre de Nigérians sont familiarisés avec ces images. M. Enwonwu est décédé en 1994.

L'ANGOLA REMPORTE

LA COUPE DU MONDE DES AMPUTÉS

BBC NEWS À BBC.CO.UK/NEWS

L'Angola a remporté la Coupe du monde de football des amputés de 2018 au Mexique, avec une victoire aux tirs au but de 5:4 sur la Turquie.

Le jeu avait abouti à un match nul 0:0 à la fin du temps réglementaire et les adversaires n'ont pas pu se départager pendant la prolongation. Les tirs au but décisifs se sont révélés tout aussi tendus, et les deux équipes ont marqué des buts avec leurs quatre premiers tirs au but.

Le football des amputés se joue avec sept concurrents dans chaque équipe, six joueurs et un gardien de but. Chaque joueur avait subi l'amputation d'une jambe et chaque gardien de but l'amputation d'un bras. Les joueurs utilisent des béquilles d'avant-bras et jouent sans prothèse.

L'Angola, qui avait fini deuxième lors de la dernière Coupe du monde, a gagné sa victoire au championnat après le tir au but décisif de Henio Guilerme.

Le Nigeria et le Kenya ont aussi représenté l'Afrique à ces jeux. Le Liberia et le Ghana, qui s'étaient aussi qualifiés pour les jeux du Mexique, se seraient retirés avant le début du tournoi après l'échec d'obtention de visa du Liberia dans les délais prescrits. Le Ghana faisait face à des difficultés financières.

Fin 2018, l'Angola était classée première parmi les 22 équipes mondiales. Le Kenya était 12ème et le Nigeria 19ème.

UNE MINE DE TALENTS REPRÉSENTÉE À LA CÉRÉMONIE DE REMISE DES PRIX

AGENCE FRANCE-PRESSE

Le Nigérian Davido a remporté le trophée AFRIMA (Prix de la musique panafricaine) de l'artiste de l'année, en tête d'une forte participation par les vedettes de l'Afrobeats d'Afrique de l'Ouest.

Des musiciens de tout le continent se sont rendus au Centre de conférence international d'Accra, capitale du Ghana, en novembre 2018 pour marcher sur le tapis rouge et célébrer une année de grands succès.

L'artiste ghanéenne Wiyaala interprète une chanson lors des Prix de la musique panafricaine de 2018.

AFP/GETTY IMAGES

L'Éthiopienne Betty G a remporté le prix de l'album de l'année et Afrotronix, originaire du Tchad, a remporté celui de meilleur DJ africain.

Le rappeur nigérian Falz a gagné le prix du meilleur rappeur après avoir relancé la polémique cette année avec la parution de *This is Nigeria* [C'est ça le Nigeria], qui discréditait le Nigeria moderne. Il était basé sur *This is America*, le succès de Childish Gambino.

Akwaaba, collaboration infectieuse entre GuiltyBeatz, Mr. Eazi, Patapaa et Pappy Kojo, a gagné les prix de meilleure chanson de l'année et meilleure collaboration africaine. Le Nigérian 2Baba a remporté le prix de la meilleure chanson pop africaine, le Ghanéen Stonebwoy celui du meilleur reggae, et le Sud-Africain Sibusiso Mashiloane celui du meilleur jazz.

Kuami Eugene, le crooner ghanéen, a été nommé l'artiste « le plus prometteur » d'Afrique.

AFRIMA s'est affirmé comme plateforme pour mettre en valeur l'industrie musicale africaine, innovante et prolifique, qui a explosé au cours de la dernière décennie. Après une carrière de 15 ans dans le secteur bancaire et le marketing, le Nigérian Mike Dada a créé ces prix comme version africaine des Grammies. L'événement de 2018 est la quatrième cérémonie.

L'Égypte et le Soudan unissent leurs forces pour sécuriser leur frontière

REUTERS

L'Égypte et le Soudan, deux pays qui font face à des menaces transfrontalières dues aux milices actives en Libye, ont convenu d'organiser des patrouilles militaires conjointes le long de leur frontière.

Ces patrouilles pourraient finalement conduire à une force conjointe dans la région frontalière pour « combattre le terrorisme et la criminalité transfrontalière, contrôler la frontière et combattre toutes les manifestations de fuite », a déclaré aux journalistes Kamal Abdul Maarouf, chef d'état-major soudanais.

Il a déclaré que les deux forces armées formeraient un partenariat stratégique dans tous les domaines, notamment ceux du renseignement, de la coopération opérationnelle et de la formation.

Les pays ont aussi convenu d'effectuer des investissements conjoints, a déclaré M. Abdul Maarouf, et d'autoriser l'Égypte à créer des projets de production agricole et de bétail au Soudan.

Une garde d'honneur soudanaise accueille le ministre égyptien de la Défense. AFP/GETTY IMAGES

Les relations entre l'Égypte et le Soudan se sont améliorées nettement malgré une tension persistante concernant le barrage sur le Nil construit par l'Éthiopie. L'Égypte considère ce projet comme une menace pesant sur son approvisionnement en eau mais le Soudan le soutient à cause de ses besoins en électricité.

Les deux pays ont un intérêt commun pour rétablir la paix en Libye, qui est déchirée par des luttes internes depuis que le dictateur Mouammar Kadhafi a été renversé en 2011. La vacance du pouvoir qui en a résulté a permis le développement des milices rivales et des groupes islamistes armés.

LE SÉNÉGAL OUVRE UNE ÉCOLE DE CYBERSÉCURITÉ

AGENCE FRANCE-PRESSE

Le Sénégal a inauguré une école de cybersécurité dans le but de renforcer les défenses d'Afrique de l'Ouest contre les hackers d'ordinateurs et d'empêcher l'Internet d'être utilisé pour financer la terreur ou disséminer la propagande.

Le ministre des Affaires étrangères sénégalais Sidiki Kaba et son homologue français Jean-Yves Le Drian ont ouvert l'école nationale de cybersécurité en marge d'une conférence annuelle sur la sécurité régionale à Dakar.

L'école formera le personnel des services de sécurité, du secteur judiciaire et des entreprises privées pour combattre la cybercriminalité. Soutenue par la France, elle aura un « rôle professionnel régional » pour aider d'autres pays d'Afrique de l'Ouest, déclarent les responsables français.

L'école, qui avait été proposée lors d'une conférence précédente sur la sécurité, sera initialement basée à Dakar à l'École nationale d'administration avant d'être relocalisée à Diamnadio, nouvelle ville en cours de construction située à une trentaine de kilomètres de la capitale.

Le Sénégal a un taux de pénétration Internet de plus de 50 % et essaie de devenir un chef de file du continent dans le domaine de la cybersécurité. Il est le premier pays à avoir ratifié la Convention de l'Union africaine sur la cybersécurité et la protection des données.

LE RETOUR DE LA MISSION DIPLOMATIQUE DES ÉTATS-UNIS EN SOMALIE

BBC NEWS À BBC.CO.UK/NEWS

Les États-Unis ont rétabli une présence diplomatique en Somalie pour la première fois depuis près de 30 ans.

Le département d'État déclare que cet événement historique reflète les progrès en sécurité accomplis par ce pays d'Afrique de l'Est. L'ambassadeur Donald Yamamoto est le chef de la mission diplomatique à Mogadiscio, qui était précédemment basée à Nairobi.

Les États-Unis avaient fermé leur ambassade de Somalie en janvier 1991 au milieu de combats entre les rebelles et le gouvernement et ils avaient dû évacuer par pont aérien leur ambassadeur et son équipe. En commentant sur ce dernier développement, la porte-parole du département d'État Heather Nauert déclare : « Notre retour démontre l'engagement des États-Unis à faire progresser la stabilité, la démocratie et le développement économique qui sont dans l'intérêt des deux nations. »

Donald Yamamoto, ambassadeur des États-Unis en Somalie, à gauche, et Mohamed Abdullahi Mohamed, président de Somalie. DÉPARTEMENT D'ÉTAT US

Le groupe extrémiste al-Shebab a été obligé de s'enfuir de la capitale en août 2011 à la suite d'une offensive lancée par les troupes de l'Union africaine. La sécurité s'est améliorée à Mogadiscio, bien que les extrémistes d'al-Shebab continuent à constituer une menace.

Avec cette présence diplomatique, l'Agence américaine pour le développement international (USAID) a annoncé de nouveaux investissements de plus de 900 millions de dollars dans le pays. Cela inclut 420 millions de dollars en assistance humanitaire, ainsi que des fonds pour les programmes axés sur la création des emplois, la bonne gouvernance, l'allègement des dettes et l'éducation.

LA MISSION DE LA CDAA AIDE LE LESOTHO À SE STABILISER

AGENCE FRANCE-PRESSE

Un Basotho à cheval suit la route qui conduit à la chaîne de montagnes Maloti au Lesotho. AFP/GETTY IMAGES

Les soldats envoyés au Lesotho en 2017 après l'assassinat du principal responsable militaire du pays se sont retirés de la région en novembre 2018. Le bloc régional de la Communauté de développement d'Afrique australe (CDAA) avait déployé une force dans ce royaume sans littoral après que des officiers d'une faction supposée rivale aient abattu un commandant militaire dans une caserne. Dans la région, on craignait une hausse de l'instabilité.

La force des sept nations de la CDAA, s'élevant à 207 militaires, 15 agents de renseignement et 24 officiers de police, fut déployée pour six mois, puis son mandat fut prolongé d'un an. La mission consistait à « renforcer la paix et la sécurité », déclare Barbara Lopi, porte-parole de la CDAA.

Lors d'une cérémonie marquant la fin de la mission, Stergomena Lawrence Tax, secrétaire exécutive de la CDAA, a salué les progrès accomplis pour restaurer la sécurité. « Il existe une amélioration considérable dans les relations de travail entre les différentes agences de sécurité, le gouvernement et la société civile », déclare-t-elle.

Le Premier ministre Thomas Thabane déclare que la mission de la CDAA prend fin au Lesotho, « confiante que nos agences de sécurité vont désormais respecter l'autorité civile et conduire leurs affaires de la façon prévue par la constitution ».

Le Lesotho, appelé la Suisse de l'Afrique du fait de ses paysages montagneux, a de longs antécédents d'instabilité politique. Il a subi des coups d'état en 1986 et 1991.

LE PRÉSIDENT DES COMORES ACCUEILLE LES RECRUES QUI ONT ÉTÉ FORMÉES

PERSONNEL D'*ADF*

La formation des soldats et des gendarmes des Comores peut être difficile : parmi les plus de 900 personnes qui se sont inscrites à un cours de formation, seulement 541 ont achevé le cours.

La formation a commencé à Itsundzu en 2018 et a pris le nom de « Feta 2018 ». La classe a formé 263 soldats et 278 gendarmes. Le président comorien Azali Assoumani a félicité les recrues lors de la remise des diplômes en février 2019 et leur a dit qu'elles avaient non seulement appris de nouvelles aptitudes techniques et tactiques, mais aussi les règles des soldats qui s'engagent à soutenir l'état de droit et les lois internationales.

Le président comorien Azali Assoumani AFP/GETTY IMAGES

Les cinq premières recrues de la gendarmerie et celles de la force de défense des Comores ont été honorées par des certificats pendant la cérémonie.

Le mufti de la république, leader religieux musulman, a aussi assisté à la cérémonie. Selon un rapport du journal comorien *Al-watwan*, le mufti a demandé aux nouveaux soldats d'assumer la responsabilité de protéger le pays, le président et le drapeau, et de travailler pour le bien du peuple.

Ce pays est un petit archipel de moins de 1 million d'habitants, qui possède des effectifs militaires et policiers de plus de 1.000 personnes.

UNE OPÉRATION CONJOINTE RÉPRIME LA CRIMINALITÉ TRANSNATIONALE

Des gendarmes burkinabés patrouillent dans la ville d'Ouahigouya au Nord du pays. AFP/GETTY IMAGES

PERSONNEL D'*ADF*

Le Burkina Faso, la Côte d'Ivoire et le Ghana ont lancé une opération de sécurité conjointe appelée Koudanlgou II dans les régions Sud et Ouest du Burkina Faso. Plus de 2.000 agents de sécurité des trois pays ont participé en novembre 2018 à l'opération, qui était conçue pour réprimer la criminalité transnationale, notamment le terrorisme, la contrebande et le trafic des stupéfiants.

Lors d'une conférence de presse après cette opération à Bouna (Côte d'Ivoire), les responsables ont déclaré qu'elle avait conduit à 150 arrestations, à la confiscation de 11 véhicules et à la saisie d'armes, de munitions, de cannabis et d'alcool, selon un rapport du site Web d'actualités burkinabé Bafujii Infos. Les forces de sécurité ont aussi offert des soins de santé à la population locale, et elles ont peint une école et réparé une route.

Le ministre de la Sécurité burkinabé Clément Pengdwendé Sawadogo déclare que l'opération a renforcé le partenariat entre les soldats des trois pays et les a aidés à coordonner leurs efforts et à mieux connaître la région frontalière des trois pays.

Le Bénin, le Burkina Faso, le Ghana et le Togo ont organisé une table ronde en mai 2018, à laquelle ont participé les chefs de la sécurité et les responsables des services appropriés, pour discuter du renforcement des relations afin de combattre la criminalité transfrontalière.

L'ARMÉE DE L'AIR ÉTHIOPIENNE *frappe al-Shebab*

PERSONNEL D'*ADF*

L'Armée de l'air éthiopienne a bombardé un campement d'al-Shebab et tué deux leaders du groupe.

Le bombardement de Bur Haybe à l'Est de Baidoa le 24 janvier 2019 a duré environ 45 minutes, selon un rapport d'Africa News citant l'Ethiopian Broadcasting Corp. Les frappes ont tué le chef des opérations régionales d'al-Shebab et un expert en explosifs, en plus de 35 combattants d'al-Shebab. Elles ont aussi détruit quatre camions militaires et cinq armes de gros calibre, selon Africa News.

Des rapports de la semaine précédente indiquaient que les troupes éthiopiennes avaient été prises en embuscade par al-Shebab à Baidoa et avaient subi des pertes.

L'Éthiopie a rejoint officiellement la Mission de l'Union africaine en Somalie (AMISOM) en 2014, bien que ses forces armées aient contribué avant cette date à l'effort régional. En février 2019, l'AMISOM a nommé le lieutenant-général éthiopien Tigabu Yilma Wondimhunegn commandant de la force de la mission des cinq nations. « Cette mission est difficile, mais nous sommes prêts à l'accomplir », déclare le général Tigabu.

Des soldats des Forces de défense nationale éthiopiennes affectés à la mission de l'Union africaine en Somalie arrivent à Kismaayo (Somalie).

CHEMINS DE L'ESPOIR

L'Ouganda est le pays le plus actif du monde

BBC NEWS À BBC.CO.UK/NEWS

Un rapport sur l'inactivité physique dans le monde révèle que l'Ouganda est le pays le plus actif du monde.

Cette étude publiée dans le journal médical *The Lancet* est une compilation d'enquêtes conduites dans 168 pays. Elle souligne les risques de santé liés au manque d'exercice.

Elle a révélé que seulement 5,5 % des Ougandais ne font pas suffisamment d'activités physiques, lesquelles sont définies comme des activités d'intensité moyenne pendant 150 minutes par semaine, ou des activités vigoureuses pendant 75 minutes par semaine.


REUTERS

Les habitants du Lesotho, du Mozambique, de la Tanzanie et du Togo ont aussi de très bons résultats en termes de temps d'exercice suffisant.

En comparaison, les habitants des Samoa américaines, de l'Irak, du Koweït et de l'Arabie saoudite semblent vivre de façon plus sédentaire. Un quart environ de la population mondiale ne fait pas assez d'exercice.

Selon ce rapport, 67 % de la population du Koweït n'est pas suffisamment active. La Mauritanie, avec 41,3 %, est le pays le moins actif de l'Afrique subsaharienne.

Comment donc s'y prend l'Ouganda ? Les habitants des zones rurales de l'Ouganda, qui représentent la majorité de la population, sont actifs dans leur ferme, déclare Patience Atuhaire de la BBC. Mais les habitants des zones urbaines sont plus sédentaires, surtout lorsqu'ils deviennent plus riches, déclare-t-elle.

Un programme offre des améliorations pédagogiques à Madagascar

BANQUE MONDIALE

Les dépenses d'éducation publique à Madagascar ont baissé en 2009 à la suite d'une crise politique, ce qui a exposé des milliers d'enfants au risque d'abandon scolaire. D'autres ont dû renoncer à leurs études parce que la famille ne pouvait plus assumer le coût de leur éducation. Avec une forte contraction du financement extérieur, les dépenses publiques en éducation ont baissé depuis 2010. Dans l'ensemble du pays, peu d'écoles ont été construites, le matériel de classe n'a pas été fourni aux enseignants et aux élèves, et beaucoup d'écoles n'ont pas reçu de financement de l'état.

Le financement d'urgence aide à restructurer l'éducation de base. Le but du Projet de soutien d'urgence à l'éducation pour tous de Madagascar est de garder les enfants dans les écoles primaires en réduisant les coûts pour les familles, en versant des subsides aux enseignants et en fournissant des trousses scolaires aux élèves.

Ce projet, lancé par la Banque mondiale en 2013, a renforcé un système d'éducation en voie d'effondrement.

À la fin de ce projet de quatre ans, il était déployé dans 12 régions malgaches et atteignait plus de 2 millions de personnes. Le projet a permis d'inscrire à l'école près de 1,9 million d'enfants, de verser le salaire de 20.000 enseignants et de distribuer plus de 5 millions de trousses scolaires. Il a permis de donner à manger à plus de 100.000 enfants dans les cafétérias des écoles des trois régions du Sud de Madagascar frappées par la sécheresse, et de construire plus de 260 salles de classe et former 50.000 enseignants.


Des élèves dans une école de la région d'Androy à Madagascar.
AFP/GETTY IMAGES

Il a posé les jalons pour le nouveau programme de soutien à l'éducation de base de 100 millions de dollars, financé par la Banque mondiale et le Partenariat mondial pour l'éducation. Ce programme améliore l'enseignement au cours des deux premières années d'école à Madagascar.

Le but du nouveau projet est d'atteindre plus de 4,7 millions de bénéficiaires. Ce chiffre inclut l'inscription de 4,6 millions d'enfants à l'école primaire et 80.000 enfants aux centres d'apprentissage précoces, et la formation de 35.000 enseignants du primaire, 6.500 éducateurs communautaires avant le primaire, 4.000 membres des commissions scolaires communautaires et 20.000 proviseurs et superviseurs locaux.

Les gosses d'Afrique du Sud apprennent le codage

AGENCE FRANCE-PRESSE

C'est mercredi à 14 heures précises dans la municipalité fortement peuplée d'Ivory Park (Afrique du Sud). L'heure est venue pour environ 60 jeunes de 11 ans de se livrer à des duels dans leur club de codage local.

Armées de blocs de codage de base, de kits d'inventeur, de portables et d'une imagination intarissable, six équipes d'école primaire entrent en compétition. Les gosses du club de codage utilisent des cartes électroniques pour fabriquer des circuits temporaires et des prototypes afin de chercher des solutions aux problèmes qu'ils ont identifiés dans leur communauté.

« Nous fabriquons un incubateur pour aider les enfants qui naissent prématurément ou ceux qui sont malades », déclare l'élève Sifiso Ngobeni. Les concurrents d'une autre école combattent le fléau des enfants disparus.

Un codage est une instruction qu'un robot ou un programme informatique lit et exécute. Dans un club de codage, les élèves apprennent à concevoir un code pour le réaliser. Bien que l'accès à l'école se soit amélioré en Afrique du Sud depuis la fin de l'apartheid, le système éducatif enregistre souvent des échecs.

« Le fait qu'il y ait toujours 80 % des enseignants qui utilisent la craie et le tableau noir aujourd'hui est une cause sérieuse de grande préoccupation », déclare l'activiste pédagogique Hendrick Makaneta. « Il ne peut pas être juste que les classes de 2018 ressemblent toujours exactement à celles de 1918. »

Dans un pays où plus de 50 % des jeunes sont au chômage, les clubs de codage améliorent aussi les chances de trouver un emploi.

Bien que la plupart des élèves d'Ivory Park soient familiarisés avec l'utilisation des smartphones, des téléviseurs connectés et de l'Internet, le codage et la compréhension des algorithmes présentent un tout autre défi.

Un rapport de 2018 de McKinsey souligne que 45 % de toutes les tâches actuelles pourraient être automatisées avec la technologie existante. D'innombrables aspects de la vie, depuis la science jusqu'à l'ingénierie, aux services financiers, au droit ou aux arts, dépendront du codage.

Des élèves travaillent avec des kits de robotique lors d'une réunion du club de robotique et de codage dans une école d'Afrique du Sud. AFP/GETTY IMAGES

UN RAPPORT INDIQUE QUE LES AFRICAINS VIVENT PLUS LONGTEMPS ET PLUS SAINEMENT

VOICE OF AMERICA

L'Organisation mondiale de la santé (OMS) déclare que les Africains vivent plus longtemps et plus sainement. Mais l'OMS avertit que des millions de personnes dans le continent affrontent toujours les défis des maladies chroniques.

L'annonce de cette amélioration a été faite lors d'une conférence à Dakar (Sénégal), où des représentants de l'OMS se sont réunis avec des responsables de 47 pays africains.

L'espérance de vie en bonne santé sur le continent (nombre d'années de vie d'une personne dans un état de santé optimal) a augmenté de 44,4 ans au début du siècle à 53,8 ans en 2015. Dans l'ensemble, l'espérance de vie a augmenté de 50,8 à 61,2 ans.

Matshidiso Moeti, directeur régional de l'OMS pour l'Afrique, déclare que deux facteurs sont principalement responsables pour ce changement. « Ce résultat est dû à une énorme augmentation de l'accès au traitement contre le VIH/SIDA et à une meilleure prévention et gestion du paludisme », déclare M. Moeti.

Mais l'OMS déclare que le type de maladie qui affecte le plus fréquemment les Africains est aussi en train de changer.

Bien que le nombre de décès provenant des maladies diarrhéiques, des infections respiratoires et du VIH soit en baisse, les conditions chroniques telles que le cancer et les maladies cardiaques font davantage de victimes.

Les taux de décès dus aux maladies non transmissibles sont restés les mêmes depuis 2000, tandis que les dix autres causes principales de mortalité en Afrique ont baissé de 40 %.

L'OMS déclare que les services de santé africains doivent s'adapter aux nouveaux défis de santé. Humphrey Karamagi, coordinateur de l'OMS, déclare que les besoins de santé des jeunes Africains sont trop souvent ignorés. « Le genre de défis de santé auxquels les adolescents font face sont très différents de ceux que nous sommes habitués à affronter : consommation des drogues, obésité des adolescents, etc. »

L'AFRIQUE CHERCHE *à développer son tourisme*

AGENCE FRANCE-PRESSE

5 % seulement des touristes mondiaux se rendent en Afrique, malgré sa promotion des attractions allant des grandes pyramides et des chutes Victoria jusqu'aux safaris d'animaux sauvages et aux étendues sans fin de plages immaculées.

Mais l'énorme potentiel du continent peut être réalisé grâce à l'écotourisme, aux expériences culturelles, aux voyages nationaux et á la stabilité politique, déclarent les experts lors d'une conférence sur le tourisme africain au Cap (Afrique du Sud).

« Lorsque vous considérez les histoires à succès, ce sont celles des pays qui adoptent les tendances », déclare Naledi Khabo, directeur général de l'Association du tourisme africain. « Lorsque vous considérez les pays qui se sont concentrés sur la durabilité, comme la Tanzanie ou le Rwanda, ceux-ci sont très attrayants pour certains voyageurs. »

Les safaris écologiques et l'hébergement neutre en carbone attirent de plus en plus de touristes d'Europe et d'Amérique du Nord. Le nombre de touristes qui visitent la Tanzanie a plus que doublé depuis 2006 pour atteindre plus de 1 million, ce qui correspond à une contribution de 14 % au produit national brut, selon le site Internet Tanzania Invest.

L'Afrique du Sud a enregistré un boom de tours basés sur les expériences alternatives, qui permettent aux voyageurs de séjourner dans les municipalités défavorisées et les communautés rurales, ainsi que dans les exploitations viticoles et les pavillons de chasse.

Le tourisme est un employeur majeur pour les Sud-Africains pauvres avec près de 700.000 emplois, succès rare dans un pays dont le taux de chômage atteint près de 27 %.

Bien que de nombreuses destinations africaines aient sollicité les devises fortes des visiteurs étrangers, le Kenya a investi intensément dans la promotion des « vacances à la maison ». Le pays s'est engagé à promouvoir les voyages nationaux lorsque les arrivées internationales ont baissé à la suite des récents troubles violents et des attaques criminelles.

« Nous avons réussi à développer le marché national », déclare Najib Balala, ministre kényan du Tourisme. « Le marché national contribue 21 % au taux d'occupation d'Airbnb. Il nous bénéficie. »

Le tourisme, qui est maintenant le deuxième facteur principal de la croissance du Kenya, représentait un chiffre d'affaires de 1,2 milliard de dollars en 2017.

Un grand nombre de pays du continent ont eu des difficultés pour attirer les visiteurs étrangers qui craignaient l'instabilité politique et la violence. Le Rwanda est un pays qui a réussi à transformer son image mondiale. Cette petite nation d'Afrique de l'Est, déchirée par le génocide de 1994, s'est depuis positionnée comme une destination haut de gamme.

« Le tourisme est le secteur qui gagne le plus de devises étrangères, ce qui est étonnant de voir dans un pays comme le Rwanda », déclare Rosette Rugamba, qui dirigeait Rwanda Tourism de 2003 à 2010. « Il contribue énormément à la promotion de l'image de notre pays. »

Le volcan du Visoke au Rwanda THE ASSOCIATED PRESS

Démonstration de dance pour les touristes à Kinigi, dans le Nord du Rwanda AFP/GETTY IMAGES

REUTERS

L'AFRIQUE DE L'EST FACILITE LE COMMERCE

VOICE OF AMERICA

Une société internationale de transfert d'argent a lancé un service en ligne pour que les habitants d'Afrique de l'Est puissent envoyer et recevoir de l'argent plus facilement. Les analystes déclarent que WorldRemit réduira le coût des transferts d'argent et stimulera les économies africaines.

L'Afrique est devenue un marché florissant pour les entreprises de transfert d'argent à mesure que ses installations de télécommunication et ses économies se sont développées.

WorldRemit, société basée au Royaume-Uni, assure le transfert d'au moins 1,6 milliard de dollars vers l'Afrique chaque année. Ismaïl Ahmed, co-fondateur et chef de WorldRemit, déclare que les transferts d'argent en Afrique ont changé au cours des années.

« Lorsque nous avons lancé nos services, 99 % des versements étaient en espèces, pour les envois aussi bien que pour les réceptions, déclare-t-il. Mais aujourd'hui, cela change rapidement, et dans les prochaines années nous pensons que jusqu'à 50 ou 60 % des versements internationaux ne se feront plus en espèces traditionnelles et passeront au numérique. C'est pourquoi nos services se sont développés très rapidement au cours des dernières années. »

M. Ahmed déclare que, à mesure que les transactions deviennent numériques, le coût de chaque transfert baisse et le suivi de l'argent devient plus facile.

« Les commerces et les personnes peuvent plus facilement envoyer [de l'argent] dans le pays, et aussi d'un pays à un autre, déclare-t-il. Il est plus facile de lutter contre le crime financier parce que, lorsque la transaction devient numérique, il existe une piste de vérification, à l'encontre de l'argent comptant qui n'est pas traçable. »

Gerrishon Ikiara, maître de conférences en affaires économiques internationales à l'Université de Nairobi, déclare que les transferts d'argent numériques vont stimuler le commerce en Afrique. Toutefois, il note que certains pays n'ont toujours pas les connexions nécessaires.

« Le défi principal concerne évidemment le niveau d'infrastructure, parce que les choses sont un peu difficiles dans un pays sans infrastructure fiable du réseau électrique et des télécommunications », déclare M. Ikiara.

LE MAROC INAUGURE LE TRAIN LE PLUS RAPIDE DU CONTINENT

REUTERS

Le Maroc a inauguré le train le plus rapide d'Afrique, qui promet de réduire de moitié le temps de voyage entre les centres commerciaux et industriels de Casablanca et Tanger.

Le roi Mohammed VI et le président français Emmanuel Macron ont pris le train pour son voyage inaugural entre Tanger et la capitale de Rabat en novembre 2018. Le train atteindra finalement une vitesse de 320 km/h, ce qui réduira fortement le temps nécessaire pour effectuer le voyage de 200 kilomètres entre les deux villes.

Il est environ deux fois plus rapide que le Gautrain grande vitesse d'Afrique du Sud, qui relie l'aéroport international de Johannesbourg à son district financier de Sandton.

L'agence de presse d'état MAP déclare que la construction de la voie ferrée a pris sept ans et a coûté 22,9 milliards de dirhams (2,4 milliards de dollars).

L'Office national des chemins de fer du Maroc, chargé de l'exploitation du réseau ferroviaire national marocain, a obtenu 12 trains grande vitesse auprès du fabricant français Alstom, selon le site Railway Technology.

Les trains sont conçus pour accommoder le climat et l'environnement du Maroc et peuvent transporter 533 passagers.

Ils sont équipés des dernières technologies afin d'assurer le confort des passagers. Ils offrent aussi aux passagers des systèmes d'informations numériques bilingues (en arabe et en français).

IMAGE DU PASSÉ

L'EMPIRE DU MONOMOTAPA

PERSONNEL D'*ADF*

Le royaume du Zimbabwe connut un déclin au début du 15ème siècle. Certains historiens disent que la famine sévissait dans la région. D'autres déclarent que Nyatsimba Mutota, prince guerrier du royaume, avait quitté cette région sans littoral à la recherche du sel, commodité précieuse à l'époque.

On dit que le prince trouva du sel parmi une tribu de chasseurs d'éléphants près du Zambèze, à environ 300 kilomètres au Nord. Il prit le contrôle de la région, qui contenait aussi quelques gisements d'or. Il occupa la majeure partie de la vallée du Zambèze et fonda l'empire du Monomotapa, appelé aussi Mutapa, en établissant sa capitale à Zvongombe.

L'historien David Chanaiwa déclare que l'empire était quelque peu officieux et dépendait du « charisme, du bien-être et de la sagesse politique » de son dirigeant. Mutota gouvernait son empire avec légèreté, en évitant de s'ingérer dans la vie de ses sujets.

Nyatsimba Mutota, roi zimbabwéen du 15ème siècle

BRITISH MUSEUM

On ne connaît pas d'historien de ce royaume, aussi existe-t-il peu d'information disponible. Mais les voyageurs portugais ont fourni des rapports sur la capitale, en décrivant comment elle était construite principalement avec de l'argile, du bois et de la chaume. La capitale était entourée d'une palissade en bois qui était tellement longue qu'il fallait environ une heure pour en faire le tour. À l'intérieur de la palissade se trouvaient trois bâtiments. Le prince avait sa cour dans l'un d'eux. Un autre abritait ses épouses et ses conseillers, environ 3.000 personnes au total. Le troisième abritait ses pages et ses gardes du corps, qui étaient recrutés parmi les jeunes hommes célibataires de tout le royaume. Ces jeunes hommes étaient formés pour servir ultérieurement comme bureaucrates ou soldats.

Mwened Matope, fils de Mutota, hérita du royaume et commença à l'élargir par une série de campagnes militaires. À son apogée, le royaume s'étendait sur toute la vallée du Zambèze. Les régions actuelles de l'Angola, de la Zambie, du Zimbabwe et d'une partie du Mozambique jusqu'à l'océan Indien faisaient partie de cet empire. Matope prit le surnom de *Mwene-Mutapa*, ce qui veut dire « seigneur des terres dévastées ». Ses vêtements royaux possédaient une houe à poignée d'ivoire, finement ouvragée, qui faisait partie de sa ceinture. Elle symbolisait la paix grâce à la capacité d'extraire les richesses de la terre. Matope expliquait clairement à son peuple qu'il était un roi d'origine divine, le « dieu du soleil ».

Il augmenta sa fortune par la taxation et le commerce à longue distance. Il établit des comptoirs le long du Zambèze. Il est presque certain qu'il fit du commerce à travers l'océan Indien, probablement avec la Chine et l'Inde.

La durée de ce royaume fut assez courte. Vers le milieu du 16ème siècle, il commença à décliner politiquement, militairement et culturellement. Son gouvernement central devint faible et fragmenté, et les gouverneurs provinciaux assumèrent davantage de pouvoir. Les leaders d'une province se séparèrent complètement du royaume. Les Portugais, qui avaient une présence de longue date dans la région, conquirent le royaume et choisirent son chef.

Lorsque les Portugais tuèrent le dernier chef du Monomotapa lors d'une bataille en 1917, le royaume était un pâle reflet de son ancienne gloire.

OÙ SUIS-JE ?

INDICES

1. Les Carthaginois ont fondé un comptoir d'échange dans ce site et il a été définitivement occupé au quatrième siècle av. J.-C.
2. Après la chute de Carthage, la ville a passé sous domination romaine. Des bains, des temples et des fontaines datent de cette époque.
3. La ville a cessé d'exister peu après la conquête arabe de 635.
4. Des fouilles ont mis au jour plus de la moitié de l'ancienne ville, y compris un théâtre.

RÉPONSE Le site archéologique de Sabratha (Libye)

PARTAGEZ VOTRE EXPERTISE

Vous désirez être publié ?

Africa Defense Forum (ADF) **est un magazine militaire professionnel** qui sert de cadre international d'échanges aux spécialistes militaires et de la sécurité en Afrique.

Le magazine est publié tous les trimestres par l'état-major unifié des États-Unis pour l'Afrique et traite des rubriques suivantes : stratégies de lutte contre le terrorisme, opérations de défense et de sécurité, criminalité transnationale, ainsi que les problèmes affectant la paix, la stabilité, la bonne gouvernance et la prospérité.

Ce cadre d'échanges permet une discussion et des échanges d'idées en profondeur. Nous voulons entendre le point de vue de personnes qui se trouvent dans nos pays partenaires africains et qui comprennent les intérêts et les défis du continent. Soumettez un article pour publication à *ADF* et faites entendre votre voix.

DIRECTIVES À L'ATTENTION DE L'AUTEUR CONCERNANT UNE SOUMISSION À *ADF*

EXIGENCES RÉDACTIONNELLES

- La préférence est donnée aux articles d'une longueur approximative de 1.500 mots.
- Les articles peuvent être remaniés pour des questions de style et d'espace. Mais *ADF* collaborera avec l'auteur sur les changements finaux.
- Incluez une courte biographie de vous-même avec vos coordonnées.
- Si possible, incluez une photographie haute résolution de vous-même ainsi que des images liées à votre article avec une légende et une mention de l'auteur de la photo.

DROITS D'AUTEUR Les auteurs conservent les droits à leur texte original. Cependant, nous nous réservons le droit de revoir et corriger les articles pour qu'ils soient conformes au style de l'Associated Press et s'intègrent dans l'espace disponible. Le fait de soumettre un article ne garantit pas sa publication. Votre contribution à *ADF* signifie votre acceptation de ces modalités.

SOUMISSIONS

Envoyez vos idées de sujet d'article, vos contenus et vos questions à la Rédaction d'*ADF* à l'adresse électronique : ***ADF.EDITOR@ADF-Magazine.com.*** Ou par courrier à l'une des adresses suivantes :

Headquarters, U.S. Africa Command
ATTN: J3/Africa Defense Forum Staff
Unit 29951
APO AE 09751 USA

Headquarters, U.S. Africa Command
ATTN: J3/Africa Defense Forum Staff
Kelley Kaserne
Geb 3315, Zimmer 53
Plieninger Strasse 289
70567 Stuttgart Germany

adf
AFRICA DEFENSE FORUM

RESTEZ CONNECTÉ

Suivez *ADF* sur Facebook et Twitter et rendez-nous visite sur le site adf-magazine.com