

adf

AFRICA DEFENSE FORUM

LA DÉFENSE CONTRE LES MENACES HYBRIDES

Comment la haute technologie et
les tactiques émergentes
mettent l'Afrique en danger



PLUS

Les groupes terroristes mettent à l'essai les drones militarisés
La promesse et le péril des réseaux sociaux

VISITEZ-NOUS SUR : ADF-MAGAZINE.COM

articles

- 8 La défense des portails du numérique**
Le piratage d'état menace l'infrastructure, l'économie et la souveraineté nationales.
- 14 La collaboration dans une guerre sans frontière**
Une conversation avec le Dr Jabu Mtsweni du Conseil pour la recherche scientifique et industrielle d'Afrique du Sud.
- 18 Le Cap oublié**
La géographie, l'histoire, la politique, les erreurs. Tout cela joue un rôle dans la montée de l'extrémisme violent dans la province mozambicaine du Cabo Delgado.
- 24 Réduire au silence la dissidence**
Les fermetures, la législation et l'influence étrangère font partie d'un effort pour censurer l'expression.
- 32 Les mines terrestres tourmentent le Zimbabwe 40 années après la guerre**
Ce pays d'Afrique australe espère éliminer ses mines en 2025.
- 38 Comment capturer un état**
Les tactiques hybrides de la Russie pour exercer un contrôle en République centrafricaine offrent un avertissement pour le continent.
- 44 Les drones peuvent être des armes mortelles pour les extrémistes**
Les terroristes emploient des drones pour identifier les cibles et conduire la surveillance en Afrique. La prochaine étape consistera à les militariser.
- 50 L'Afrique affronte des ennemis à haute technologie**
Les extrémistes emploient la technologie, les réseaux sociaux et même les jeux vidéo dans leurs attaques.



rubriques

- 4 Point de vue
- 5 Perspective africaine
- 6 L'Afrique aujourd'hui
- 30 Battement du cœur de l'Afrique
- 56 Culture et sports
- 58 Point de vue mondial
- 60 Défense et sécurité
- 62 Chemins de l'espoir
- 64 Croissance et progrès
- 66 Image du passé
- 67 Où suis-je ?



**Africa Defense Forum
est disponible en ligne.**

Veillez nous rendre visite sur le
site adf-magazine.com



SUR LA COUVERTURE :

Le continent affronte une gamme de menaces non traditionnelles, notamment les cyberattaques, les drones et la guerre de l'information. Les professionnels de la sécurité doivent se préparer à affronter ces menaces hybrides.

ILLUSTRATION D'ADF

Ce sont parfois les menaces inattendues qui provoquent le plus de dégâts. Une cyberattaque peut paralyser le réseau électrique d'une nation. La désinformation peut envoyer les manifestants dans les rues et alimenter les troubles civils. Les petits drones commerciaux peuvent causer des explosions de bombe létales.

Ces attaques, appelées menaces hybrides, sont difficiles à détecter ou à attribuer à un groupe spécifique. Souvent, des acteurs intermédiaires exécutent les attaques pour dissimuler leur origine. Elles semblent être provoquées par une petite bande de criminels locaux, mais c'est en réalité une puissance étrangère ou un groupe extrémiste qui dirige les événements à distance.

Ces attaques non traditionnelles deviennent l'outil de choix pour les groupes qui souhaitent avoir un grand impact à un coût faible. Les professionnels de la sécurité doivent être préparés.

L'Afrique par exemple, avec plus de 500 millions d'utilisateurs de l'Internet, est un terrain fertile pour les cybercriminels. Ces cyberattaques, souvent de petite échelle, ont coûté au continent une somme estimée à 4 milliards de dollars en 2021 et ont réduit le produit intérieur brut des états de 10 %.

Mais les cyberattaques représentent une préoccupation plus que simplement économique. Elles sont aussi un problème sécuritaire.

Au cours de l'année passée, le système informatique qui exploite les plus grands ports et chemins de fer commerciaux d'Afrique du Sud a été attaqué. Les agences gouvernementales sont sujettes à des attaques répétées par des logiciels de rançon. Sur le continent, les hackers visent l'infrastructure critique et les données des gouvernements.

De même, les puissances étrangères utilisent des campagnes de désinformation basées sur le numérique pour déstabiliser les pays vulnérables. La Russie, qui a envoyé des mercenaires en République centrafricaine, en Libye et au Soudan, soutient ses combattants avec des campagnes de radio, télévision et Internet. Ces campagnes sont conçues en général pour provoquer la colère et la confusion dans les pays ciblés afin de faire avancer les intérêts russes.

Finalement, la prolifération de la technologie peu chère des drones possède d'innombrables applications précieuses lorsqu'elle est utilisée pour la science, la surveillance ou la livraison des biens. Mais les groupes extrémistes ont l'intention d'employer les drones pour lancer des attaques avec des engins explosifs improvisés. Les terroristes utilisent déjà cette tactique au Moyen-Orient, avec des résultats dévastateurs. Les observateurs pensent que tôt ou tard les extrémistes emploieront les mêmes tactiques en Afrique.

Les professionnels africains de la sécurité se précipitent pour répondre à ces menaces. L'éducation militaire continue et les classes d'aptitudes seront cruciales pour cet effort, tout comme la capacité d'adopter la nouvelle technologie. Une

génération de jeunes soldats versés en informatique souhaite vivement jouer un rôle directeur dans ce combat.

La créativité et la motivation de nos adversaires pour développer de nouveaux modes d'attaque sont illimitées. Mais il en est de même pour notre résolution à vaincre ces menaces. En nous appuyant sur la formation, sur des partenaires forts et sur une capacité d'adaptation, il n'y a pas de menace que nous ne puissions pas anticiper et arrêter.

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



Des soldats à l'école d'ingénieurs militaires de l'Armée de terre nigériane à Makurdi pratiquent la détection et le désarmement des engins explosifs improvisés.

FORCE OPÉRATIONNELLE D'EUROPE DU SUD POUR L'AFRIQUE



Les menaces hybrides Volume 15, 2ème trimestre

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 USA

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.

Assurer la sécurité entre voisins



Le président Mokgweetsi Masisi du Botswana s'est exprimé devant les soldats des Forces de défense du Botswana à l'aéroport international Sir Seretse Khama de Gaborone le 26 juillet 2021,

alors qu'ils se préparaient à partir pour une affectation à la mission de la Communauté de développement d'Afrique australe au Mozambique. Ses remarques ont été modifiées pour les adapter au présent format.



Les membres des Forces de défense du Botswana écoutent le président Mokgweetsi Masisi à l'aéroport international Sir Seretse Khama de Gaborone avant de partir pour le Mozambique.

BUREAU DU PRÉSIDENT, RÉPUBLIQUE DU BOTSWANA

Je me présente devant vous comme commandant-en-chef des Forces de défense du Botswana

[BDF] et président en exercice de l'organe sur la politique, la défense et la sécurité de la CDAA [Communauté de développement d'Afrique australe]. C'est une institution officielle de la CDAA qui a été lancée en juin 1996, avec un clair mandat de soutien au succès et au maintien de la sécurité et de l'état de droit dans la région.

Aujourd'hui, ce mandat est mis à l'épreuve par un environnement géopolitique et un panorama sécuritaire qui ne sont pas différents de ceux des années formatrices de notre pays pendant la période du régime minoritaire d'apartheid. Pour autant que la situation sécuritaire dans la région de la CDAA soit complexe, comme par le passé, les objectifs de la politique étrangère du Botswana ont été et restent tout à fait clairs. La sécurité du Botswana ne pourra jamais être obtenue sans celle de ses voisins. Lorsque le Botswana a assumé le leadership de l'organe sur la triade de la politique, la défense et la sécurité de la CDAA, j'ai défini le rôle de notre pays pour diriger les efforts de la région visant à soutenir la stabilité en politique, défense et sécurité par l'application de notre capital diplomatique et sécuritaire universel aux problèmes fâcheux de notre région.

Aujourd'hui, nous constatons un autre jalon dans nos objectifs visant à encourager l'agenda de paix dans notre région, dans le

sillage du mandat de la CDAA pour faciliter des conditions pacifiques dans la région Nord de la République du Mozambique, en particulier au Cabo Delgado. C'est pour cette raison que je suis ici ce matin et je m'adresse aux membres des Forces de défense du Botswana qui, dans le cadre de leur participation à la Force en attente de la CDAA, seront déployés pour fournir un appui régional au Mozambique afin de combattre la menace émergente du terrorisme et les actes d'extrémisme violent dans la région du Cabo Delgado au Nord de ce pays, en tant qu'élément de SAMIM, la mission de la CDAA au Mozambique.

Comme précisé antérieurement, notre engagement envers la paix régionale et internationale en tant que pays reste inébranlable et intact, comme le prouve la participation enviable précédente des BDF dans les actions de maintien de la paix de l'opération Restore Hope en Somalie, d'UNOMOZ I et II [opération des Nations unies au Mozambique], dans le cadre de la mission d'observation de l'ONU au Rwanda et de Boleas au Lesotho.

Dans tous ces déploiements, les BDF ont reçu une évaluation très positive de leur conduite professionnelle dans l'exécution de leurs efforts militaires et aussi en tant qu'ambassadeurs vrais et sincères des valeurs nationales historiques et durables du Botswana et tant que société basée sur l'état de droit. Ceci reste l'héritage historique de vos prédécesseurs, dont vous devez prendre maintenant la place, chacun de vous. Je vous implore donc

tous à émuler ces prédécesseurs qui ont participé aux missions de paix précédentes, en démontrant le plus haut degré de professionnalisme pendant ce déploiement, en tant que porte-drapeau du Botswana au Mozambique.

En tant que commandant-en-chef, je sais que vous affronterez un ennemi trompeur qui utilisera probablement la guerre asymétrique, les tactiques de guerre non conventionnelles et sournoises, contre vous et la population que vous protégez. Comme professionnels, vous représentez quelque chose de beaucoup plus grand qu'eux et vous devez éviter de les imiter et de tomber à leur niveau. Et certes, toute votre formation sera très concrètement employée.

J'exige donc de vous rien moins que d'observer les lois sur les conflits armés telles que prescrites internationalement dans votre profession militaire, ainsi que l'accord de l'état des forces qui définit la structure en vertu de laquelle le personnel de la SAMIM agira au Mozambique. Je suis absolument convaincu que vous exécuterez votre tâche équitablement et ne ferez rien qui ternira la bonne image des Forces de défense du Botswana.

LES CULTIVATEURS D'ARACHIDES DE LA RCA FONT FACE AUX MENACES ET AU VOL

HISTOIRE ET PHOTOS PAR L'AGENCE FRANCE-PRESSE

Pour de nombreux cultivateurs d'arachides dans la région de Paoua (République centrafricaine), la vie est une lutte quotidienne. Ils doivent relever les plantes du sol, récolter les noix et les décortiquer. Puis, ils doivent survivre aux vols, aux extorsions ou pire dans une région où les rebelles et les forces pro-gouvernementales se font la guerre.

Jean-Paul Ndopaye, gérant d'un magasin d'arachides, a déclaré à Africanews : « C'est l'insécurité qui nous empêche de développer davantage nos récoltes d'arachides à Paoua. Lorsque nous voulons envoyer nos produits à Bangui, à Berbérati ou même à Bouar, nous pourrions rencontrer des brigands sur la route. »

Célestine Inforo, âgée de 33 ans, décortique des arachides avec une douzaine d'autres personnes dans les faubourgs de Paoua, ville de 40.000 habitants. Elle déclare : « Il y a trop de menaces et de vols. Nous avons dû vendre notre production très rapidement et à bas prix. »

Ses collègues et elle remplissent chacune plusieurs sacs en quelques heures, puis ceux-ci sont acheminés avec un attelage de deux bœufs vers un entrepôt sécurisé prêté par l'organisation non gouvernementale Oxfam. Hors de l'entrepôt, chaque sac est pesé et enregistré avec un poids entre 35 et 45 kilos.

Dans la ville, un sac d'arachides décortiquées vaut environ 10.000 francs CFA (environ 17 dollars). Dans la capitale de Bangui, un sac se vend entre 20.000 et 30.000 francs CFA, déclare Jean-Paul Ndopaye, président de l'Union des riziculteurs de Paoua.

La production dépasse fortement la demande dans la région, ce qui fait baisser les prix, et 80 % de la population de la ville travaille dans l'industrie de l'arachide.

La RCA est en proie à une guerre civile depuis 2013.



Des hommes pèsent un sac d'arachides à Paoua (République centrafricaine). Un sac pesant 35 à 45 kilos se vend pour 10.000 francs CFA environ, soit 17 dollars.

L'intensité du conflit a diminué au cours des récentes années, mais elle est remontée à nouveau pendant les dernières élections présidentielles de la fin 2020.

À l'ombre d'un manguier, les femmes transforment les arachides en huile, beurre et « kuli-kuli », bâtonnets à haute teneur nutritive. L'une d'elles fait rôtir les noix. Une autre malaxe le beurre d'arachide sur une planche en bois.

Mahoua Coulibaly, directrice locale du Programme alimentaire mondial, déclare : « C'est le traitement qui pose un problème. C'est là que des investissements doivent être faits pour le bien-être de la population, mais pour le moment il n'y a pas de fonds. »

Les enfants ougandais retournent à l'école après presque 2 ans

PERSONNEL D'ADF

L'Ouganda a mis fin à la fermeture scolaire la plus longue du monde le 10 janvier 2022 en ordonnant à des millions d'élèves de retourner à l'école, après presque deux ans pendant lesquels l'enseignement avait été suspendu à cause du Covid-19.

Les élèves sont retournés aux écoles qui étaient fermées depuis mars 2020, lorsque le Covid-19 se répandait sur la planète.

« Je suis très heureuse parce que l'école, mes professeurs, mes amis, mes études, tout cela me manquait », a déclaré Nawilah Senkungu, âgée de dix ans, à l'Agence France-Presse (AFP) dans l'école primaire Nakasero de Kampala, où les enseignants ont encouragé les élèves à porter le masque et se laver les mains.

Le ministre de l'Éducation John Musingo déclare que tous les élèves de primaire et de secondaire suivront des classes à un niveau d'une année de plus que les classes qui avaient été suspendues.

« Toutes les écoles ont mis en œuvre des consignes et des procédures opérationnelles standards pour assurer le retour en toute sécurité des enfants dans les écoles, et des mesures ont été prises pour assurer que ceux qui ne se conforment pas le fassent », a déclaré M. Musingo selon Taarifa, service de presse rwandais.

Malgré ces assurances, certains parents ont été prudents dans le sillage des infections continues. Une semaine après la réouverture, certaines écoles avaient moins de 50 % des élèves régulièrement inscrits, selon The Independent de l'Ouganda.

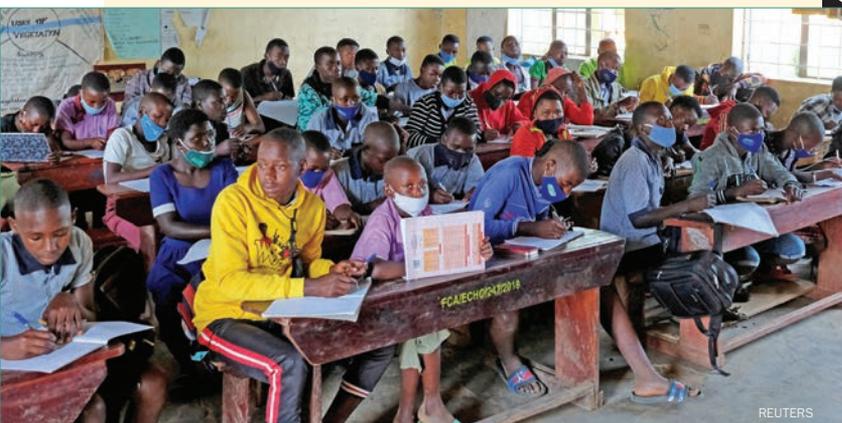
Certains administrateurs déclarent que les parents ont retenu leurs enfants pour éviter de payer les frais de scolarité jusqu'à ce qu'ils puissent être assurés de la sécurité des enfants. Dovicko Kisembo, enseignant principal de l'école secondaire Mubuku Valley dans la municipalité de Mubuku, a dit à The Independent que de nombreux parents craignent que les autorités n'annoncent un autre confinement à cause du nombre de cas de Covid-19 en hausse.

M. Musingo a dit que toute école qui exigerait des frais de scolarité supérieurs aux frais pré-pandémiques serait sanctionnée.

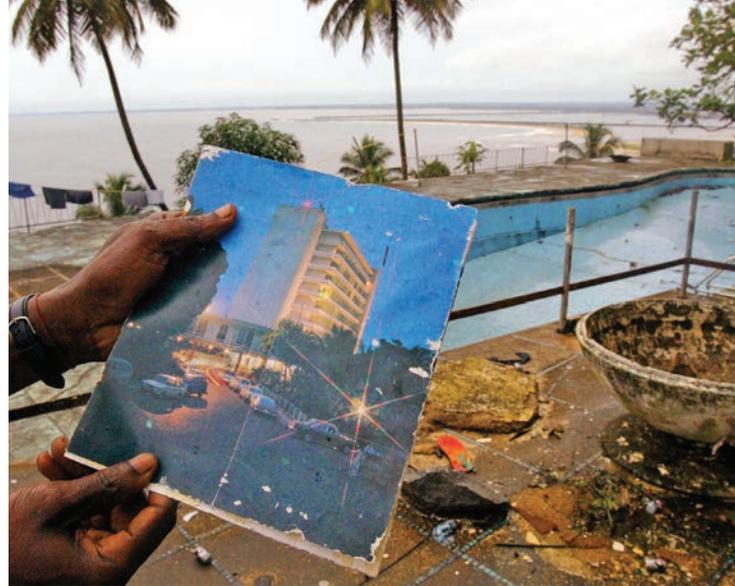
La fermeture a affecté au moins 10 millions d'élèves du primaire et du secondaire et a duré 83 semaines, selon l'UNESCO, organisme éducatif et culturel des Nations unies.

Nawilah a passé la longue période de fermeture à s'occuper des poulets et à cultiver les champs sur la petite ferme de ses grands-parents.

« Je suis très heureux de voir que mes enfants sont retournés à l'école », déclare à l'AFP Siraj Senkungu, son père. « Leurs professeurs leur ont manqué, et aussi l'enseignement. »



Les élèves travaillent sur des leçons en janvier 2022 à l'école primaire Sweswe dans l'Ouest de l'Ouganda après la réouverture des écoles.



CE VIEIL HÔTEL EST UN SOUVENIR douloureux du passé du Liberia

AGENCE FRANCE-PRESSE

Lorsqu'il avait ouvert ses portes en 1960, l'hôtel Ducor de Monrovia (Liberia) était l'un des seuls hôtels 5 étoiles d'Afrique, avec une boîte de nuit et des chambres climatisées, selon les guides de voyage.

Il a accueilli des VIP tels que l'ancien empereur d'Éthiopie Haïlé Sélassié. Les clients flânaient près de la piscine, sirotaient des cocktails et observaient les couchers de soleil sur l'océan Atlantique.

Le Ducor a fermé ses portes en 1989 au déclenchement des guerres civiles consécutives, l'une de 1989 à 1997 et l'autre de 1999 à 2003. Il est devenu rapidement délabré.

« Cela attriste tout le monde », déclare Ambrose Yebea, ex-officiel du ministère du Tourisme (à la retraite) qui offrait précédemment des visites guidées de l'hôtel.

De nombreux leaders africains sont restés au Ducor dans les années 60 et 70 ; plusieurs ont réservé des chambres lors de la conférence de 1979 de l'Organisation de l'unité africaine à Monrovia.

En 2011, Ellen Johnson Sirleaf, présidente à l'époque, a transféré le Ducor à la Libyan African Investment Co. (LAICO), filiale du fonds souverain de Libye, dans le cadre d'un plan de rénovation.

Selon une déclaration du gouvernement en 2011, l'hôtel rénové aurait 151 chambres, des restaurants, un centre commercial, un court de tennis et un casino, et il fournirait des emplois.

Toutefois, le projet qui avait un prix de 65 millions de dollars, y compris le développement d'une usine de traitement du caoutchouc, n'a pas abouti. Le Liberia a rompu ses liens avec la Libye en 2011 alors que ce pays sombrait dans la guerre civile. Les travaux de rénovation se sont arrêtés.

« Ça nous a donné un grand choc », déclare Frank Williams, ouvrier qui déclare être l'une des 150 personnes employées par LAICO. « Aujourd'hui, nous sommes au chômage. »

Le projet a été gelé depuis et son avenir est incertain. D'aucuns espèrent toujours que le Ducor renaisse. M. Yebea, l'officiel de tourisme à la retraite, dit qu'il pourrait attirer les touristes et fournir des emplois.

« Tous les Libériens le considèrent de la même façon, dit-il. Ils veulent qu'il soit restauré. »

Une brochure montre l'hôtel dans toute sa splendeur d'autrefois.

AFP/GETTY IMAGES



La défense

des

PORTAILS

du

NUMÉRIQUE

Le piratage d'état menace l'infrastructure, l'économie et la souveraineté nationales

PERSONNEL D'ADF

Les grues qui déchargent les conteneurs des navires dans deux des ports les plus affairés d'Afrique du Sud se sont presque arrêtées en juillet 2021. Les camions ont attendu pendant 14 heures ou plus pour charger leur cargaison. Les navires ont été forcés de jeter l'ancre à l'extérieur du port pendant plusieurs jours et décider s'ils ne devraient pas simplement éviter les ports affectés. Les commerçants et les consommateurs étaient préoccupés par les étagères vides à l'approche d'une saison majeure de ventes.

Denys Hobson, analyste de la logistique et des prix à la banque sud-africaine Investec, a déclaré : « Ceci n'aurait pas pu se produire à un pire moment. Si rien ne peut entrer ni sortir du pays, les conséquences économiques seront sérieuses. »

La perturbation a été provoquée par une attaque cybernétique. Les hackers avaient infiltré le réseau de Transnet, société d'état

qui gère les ports de Durban, du Cap et d'ailleurs, ainsi que les réseaux ferroviaires et de pipelines d'Afrique du Sud. Incapable de satisfaire à ses obligations contractuelles pendant plus d'une semaine, la société a été forcée de suspendre ses contrats jusqu'à la résolution de l'attaque.

Des reportages indiquent que « Death Kitty », groupe de hackers basé en Europe de l'Est ou en Russie, a revendiqué l'attaque en utilisant une technique appelée couramment le logiciel de rançon, parce qu'il gèle les systèmes informatiques jusqu'à ce qu'une rançon soit payée.

C'était l'attaque la plus grave jamais commise contre l'infrastructure critique d'Afrique du Sud, mais les experts avvertissent que ce ne sera pas la dernière.

Denys Reva écrit pour l'Institut pour les études de sécurité : « Il est probable que les attaques contre l'infrastructure critique, y compris les ports maritimes, augmenteront

« Il est probable que les attaques contre l'infrastructure critique, y compris les ports maritimes, augmenteront en gravité et en nombre. » ~ Denys Reva, Institut pour les études de sécurité

en gravité et en nombre. Les pertes économiques pour les états africains seront inévitablement élevées, ce qui veut dire que les mesures visant à renforcer la cybersécurité et protéger l'infrastructure sont vitales. »

Un pays sujet à des risques

Au premier trimestre 2021, l'Afrique du Sud a été frappée par des attaques de logiciel de rançon plus durement que tout autre pays du continent, selon le Rapport d'évaluation des cyber-menaces africaines d'Interpol.

Les agences gouvernementales sont parmi les entités les plus ciblées.

En septembre 2021, une attaque a forcé le département de la Justice et du Développement constitutionnel d'Afrique du Sud à mettre hors service son système de technologie de l'information (TI) qui sauvegarde les informations, y compris les fichiers personnels. Au cours d'un incident séparé pendant la même année, l'école nationale de gouvernement a dû mettre son système TI hors service pendant deux mois, ce qui a fait perdre à cette institution de formation gouvernementale environ 2 millions de rands (121.000 dollars). Même le président du pays a été affecté par des hackers qui ont infiltré son téléphone.

Les experts en cybersécurité avertissent que les institutions gouvernementales d'Afrique du Sud sont désormais directement visées par les hackers.

« La combinaison d'une technologie vieillissante, d'un financement inadéquat et d'un manque de formation, à laquelle s'ajoutent les données de grande valeur détenues par ces organisations, en fait une mine d'or pour les acteurs malveillants », écrit Saurabh Prasad pour la société sud-africaine IT-Online.

Interpol a déterminé que les organisations africaines avaient constaté une hausse de 34 % des attaques par logiciel de rançon au premier trimestre 2021, le chiffre le plus élevé au monde. Les institutions gouvernementales sont restées à la traîne pour protéger leur infrastructure IT et elles doivent se rattraper, déclare M. Prasad.

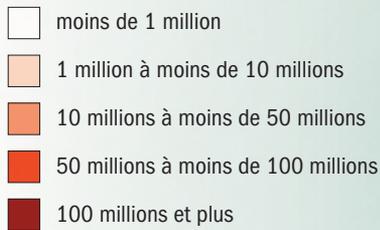
« Le panorama des menaces évolue aussi beaucoup plus rapidement que la capacité des organisations gouvernementales à effectuer des actualisations technologiques, ce qui les transforme en cibles faciles et rentables, et par conséquent très attrayantes. »

Les camions et les cargos font la file au port de Durban après une attaque cybernétique contre la société d'état Transnet en juillet 2021.

AFP/GETTY IMAGES

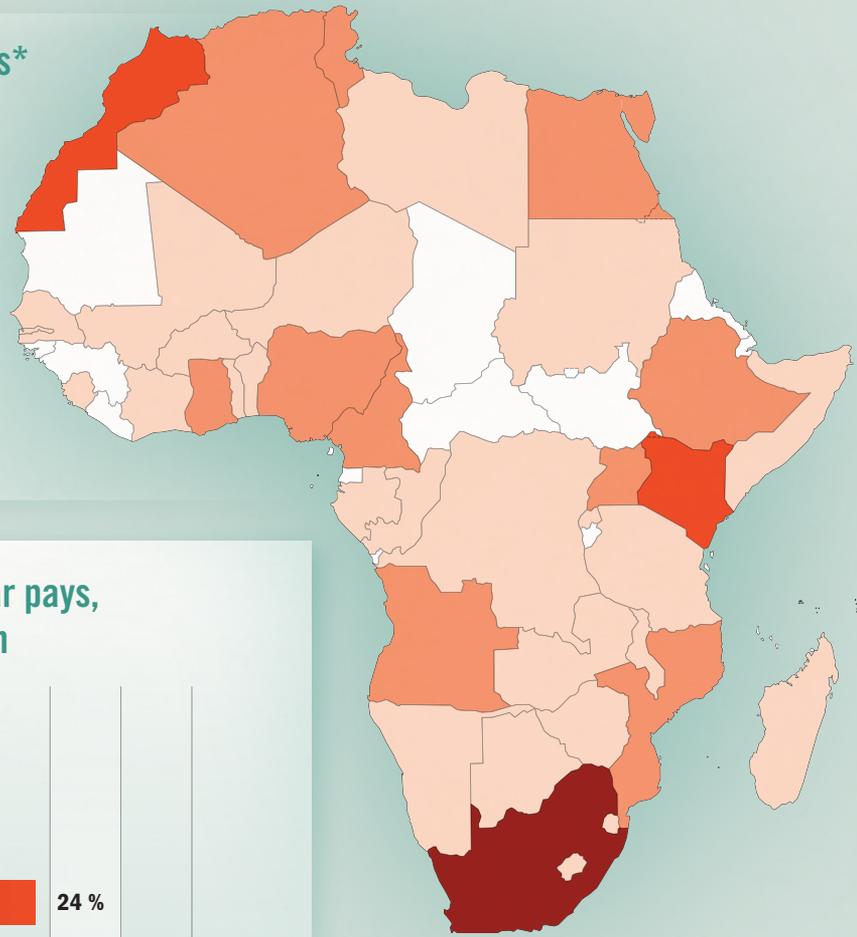


Détection des menaces par pays*

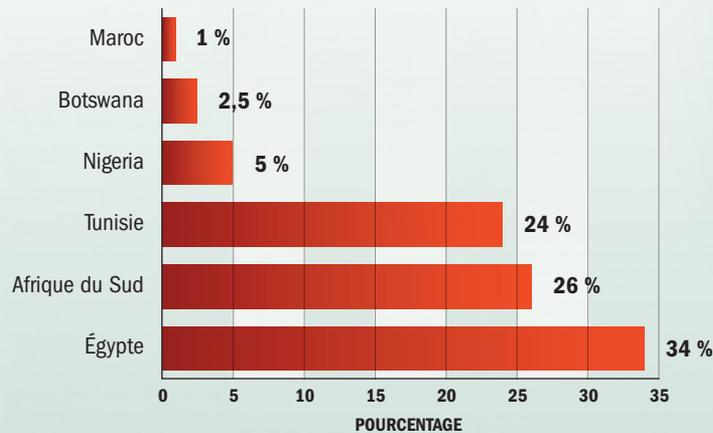


Source : Trend Micro

*Nombre de menaces détectées dans les fichiers, e-mails ou URL entre janvier 2020 et février 2021, tel que relevé par Trend Micro, société de logiciels de cybersécurité qui a un partenariat avec Interpol.



Logiciels de rançon détectés par pays, en pourcentage du total africain



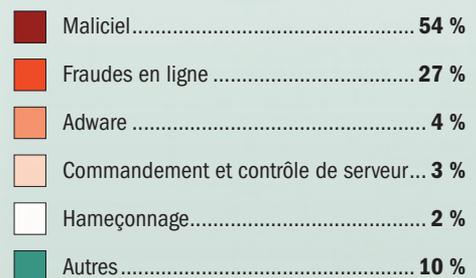
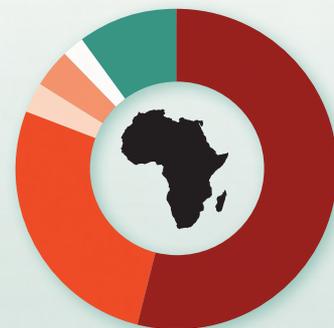
Source : Trend Micro, 2021

Un navire est ancré hors du port du Cap après une cyberattaque qui a frappé le port en 2021.

AFP/GETTY IMAGES



Menaces les plus fréquemment détectées en Afrique



Source : Trend Micro, 2021

Un navire décharge des conteneurs au port du Cap.

AFP/GETTY IMAGES



La guerre cybernétique soutenue par les états

La question de savoir si un pays quelconque ou ses agents étaient impliqués dans l'attaque de Transnet demeure incertaine, mais le piratage soutenu par les états est une menace croissante en Afrique.

En 2018, des hackers soutenus par la Chine ont volé les e-mails et les données de surveillance des serveurs situés au siège social de l'Union africaine à Addis-Abeba (Éthiopie). En 2017, des hackers soutenus par la Corée du Nord ont conduit une attaque globale appelée Wannacry qui a paralysé les entreprises et les institutions publiques de 150 pays. En 2020, des hackers égyptiens ont attaqué des entreprises et agences gouvernementales éthiopiennes en essayant de perturber la construction du Grand Barrage de la renaissance éthiopienne.

En 2021, Google a envoyé plus de 50.000 avertissements à des détenteurs de compte du monde entier en leur disant qu'ils avaient été ciblés par des tentatives de hameçonnage ou de maliciel soutenues par un gouvernement. L'un des contrevenants les plus prolifiques au monde est un groupe appelé APT35 ou « Charming Kitten », qui est lié au corps des Gardiens de la révolution islamique d'Iran.

Les pays africains sont particulièrement vulnérables face à une interférence externe. Les sociétés chinoises ont construit environ 80 % des réseaux de télécommunication du continent. La société de télécom Huawei, qui a des

liens étroits avec le Parti communiste chinois, est positionnée pour construire une grande partie du réseau 5G du continent. En outre, les sociétés chinoises ont construit des systèmes TI dans au moins 186 édifices gouvernementaux en Afrique, notamment les palais présidentiels, les ministères de la défense et les bâtiments parlementaires, selon un rapport de Heritage Foundation.

Les experts déclarent que cette infrastructure signifie que les espions pour le compte de la Chine auraient peu de problèmes à accéder aux données gouvernementales sensibles.

« Le gouvernement chinois a de longs antécédents de pratique de tous les types de surveillance et d'espionnage dans le monde », déclare Joshua Meservey, analyste principal de politique pour l'Afrique à Heritage Foundation. « Nous savons donc que c'est le genre de chose qu'ils veulent faire, le genre de chose qu'ils sont capables de faire. Et aussi que l'Afrique est suffisamment importante pour qu'ils le fassent. »

Il y a plusieurs mesures stratégiques que les pays africains peuvent prendre pour se protéger contre les cyberattaques. En voici quelques-unes :

Ériger des protections ponctuelles

À mesure que les pays développent leurs affaires en ligne et que les secteurs tels que les transports, l'eau et l'électricité sont contrôlés numériquement, les hackers décèlent

des opportunités pour causer des dommages. Les pays qui ont les taux les plus élevés de pénétration Internet ont tendance à être les plus vulnérables. Dans un sens, ceci est un avantage pour les pays africains parce que beaucoup d'entre eux ont assez tardé avant d'adopter la technologie du numérique. Cela leur donne l'opportunité d'ériger des protections alors qu'ils développent leur infrastructure TI.

Les chercheurs Nathaniel Allen du Centre africain pour les études stratégiques et Noëlle van der Waag-Cowling de l'Université de Stellenbosch en Afrique du Sud déclarent que les pays en développement ne possèdent pas le fardeau d'une ancienne architecture logicielle ou d'un « code hérité » qui est très facile à attaquer.

En établissant de bonnes pratiques dès le début, les pays qui sont moins avancés du point de vue numérique peuvent « sauter par dessus » ceux qui ont atteint un certain stade de maturité, écrivent-ils.

Diversifier les fournisseurs, bâtir une capacité interne

Les pays qui dépendent fortement d'un seul fournisseur de services externe pourraient ouvrir la porte au piratage étatique. Selon une estimation, Huawei a fabriqué 70 % des

stations de base 4G utilisées sur le continent. La société est aussi un chef de file dans les systèmes de surveillance et de reconnaissance faciale vendus en Afrique.

Alors que les projets d'infrastructure soutenus par la Chine ont proliféré sur le continent, ils sont souvent associés au développement TI qui connecte le contrôle de multiples secteurs tels que l'eau, l'électricité et les transports.

Dans un article pour le Comité international de la Croix-Rouge (ICRC), le professeur Waag-Cowling écrit : « Ceci pourrait potentiellement créer des entrées clandestines et des voies de vulnérabilité. Le résultat direct est, en pratique, la possibilité d'une perte future de contrôle souverain de l'infrastructure de communication, d'énergie, de transport ou d'eau. »

Les experts ont encouragé les pays africains à cultiver des relations avec un éventail diversifié de fournisseurs de services TI pour éviter l'écueil du fournisseur unique. La concurrence non seulement s'oppose au piratage étatique, mais elle conduit aussi à un meilleur service pour la clientèle.

Un grand nombre de pays africains essaient de développer une capacité interne dans le secteur TI. Safaricom, plus grande société de téléphone mobile du Kenya, et la société sud-africaine MTN en sont des exemples de choix.

Huawei, géant chinois des télécommunications, a fabriqué la majorité des stations de base 4G utilisées en Afrique. Les experts déclarent que cette domination et les liens étroits de la société avec le gouvernement chinois font augmenter les risques de piratage et de surveillance. AFP/GETTY IMAGES

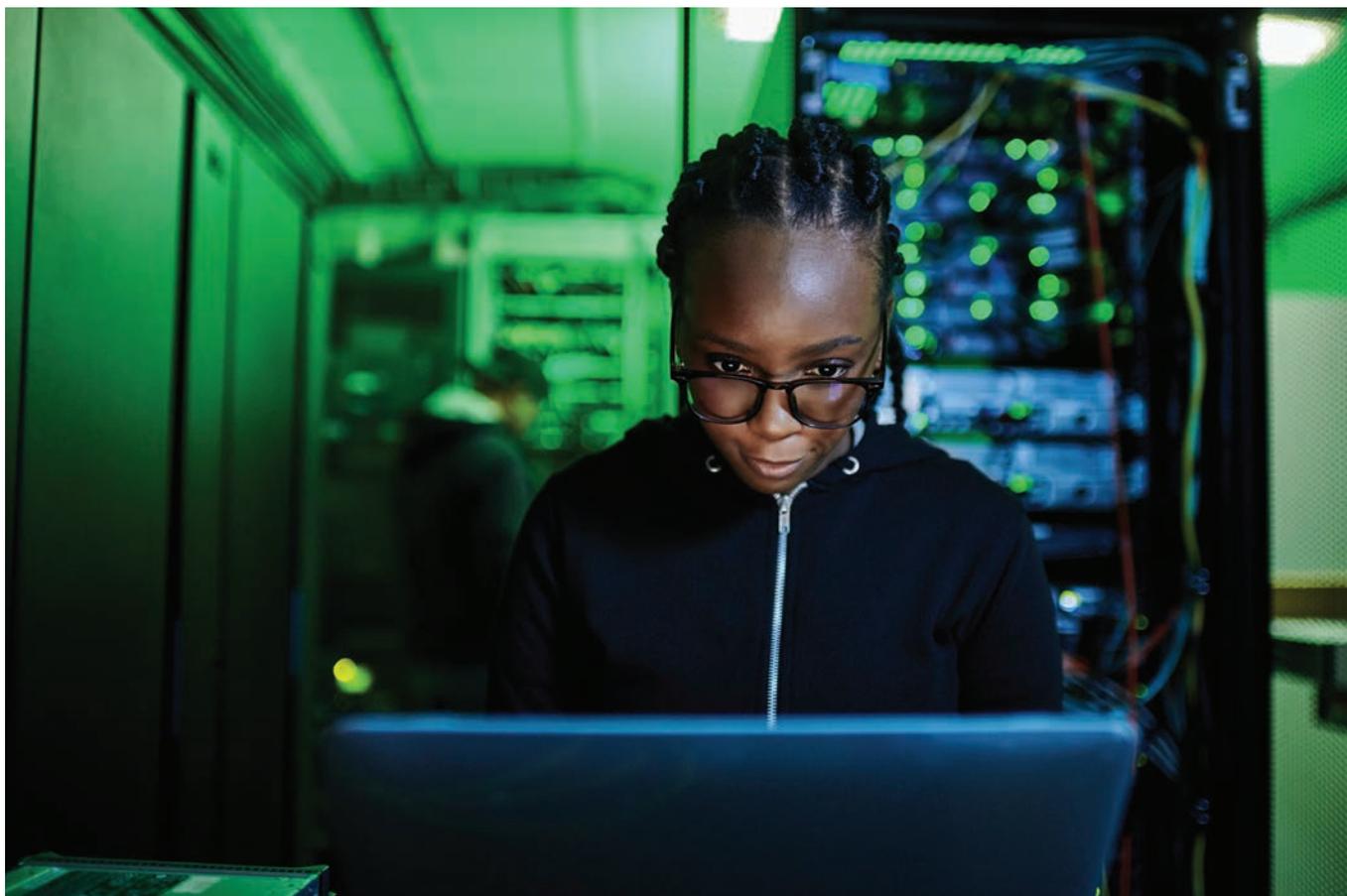
Éliminer les points de défaillance uniques

Les experts cybernétiques se plaignent que trop de systèmes TI qui contrôlent l'infrastructure critique d'un pays ont des points de défaillance uniques. Ceci veut dire que lorsqu'un serveur, un réseau ou une usine est frappé par une attaque, l'ensemble du pays peut se retrouver sans service vital comme l'eau ou l'électricité. Les défenseurs exhortent les pays africains à intégrer des redondances ou des systèmes de secours pour éviter la perte catastrophique de service pendant une attaque.

Les Nations unies et Interpol ont déclaré dans un « Recueil de bonnes pratiques » visant à se protéger contre les attaques cybernétiques : « Une seule attaque contre un point de défaillance unique pourrait conduire à la perturbation ou la destruction de multiples systèmes vitaux directement affectés dans le pays, et avoir des répercussions mondiales. Ceci crée une cible attrayante pour ceux qui ont l'intention de nuire. Et alors que nos villes et notre infrastructure évoluent, il en est de même pour leurs armes. »

Huawei s'est positionnée pour bâtir la majorité de l'infrastructure 5G en Afrique. 5G est la prochaine génération de téléphones mobiles, tours et autre technologie de soutien en cours de développement. AFP/GETTY IMAGES





Investir dans la détection/ les capacités offensives

Un grand nombre de pays investissent dans des équipes de réponse aux urgences informatiques qui peuvent surveiller les réseaux nationaux importants et l'infrastructure critique. Elles sont parfois appelées les premiers intervenants d'un pays en cas de cyberattaque.

Certains pays tels que le Nigeria créent des commandements cybernétiques au sein de leurs forces armées. Les experts déclarent qu'il est important pour ces commandements de développer des capacités défensives et offensives qui leur permettent de se protéger contre les attaques et dégrader ce qui constitue une menace avant qu'une attaque ne puisse être lancée.

L'UA a assumé un rôle de leadership pour encourager les capacités cybernétiques avec son groupe d'experts en cybersécurité, mais les observateurs préconisent une plus grande coopération régionale. Le professeur Waag-Cowling déclare que les pays africains pourraient considérer cela comme le « maintien de la paix cybernétique » par lequel les nations œuvrent ensemble pour renforcer la cybersécurité en ses points les plus faibles. Elle pense que les forces armées, en particulier leurs éléments les plus jeunes et les mieux éduqués, peuvent jouer un rôle de premier plan.

« L'expérience continue des forces armées africaines

« L'expérience continue des forces armées africaines avec les conflits irréguliers persistants pourrait fournir une plateforme pour pivoter vers des menaces de guerre hybride. »

~ Noëlle van der Waag-Cowling, Université de Stellenbosch, Afrique du Suda

avec les conflits irréguliers persistants pourrait fournir une plateforme pour pivoter vers des menaces de guerre hybride, écrit-elle pour ICRC. Une population jeune, urbanisée et technologiquement capable doit appuyer les stratégies futures de défense cybernétique. »

Les enjeux sont élevés. Le professeur Waag-Cowling avertit que, si les pays africains sont considérés comme des cibles vulnérables, les hackers les attaqueront.

« La cyberdéfense dépend dans une certaine mesure de l'estimation par les attaquants que la capacité d'un état à riposter aux attaques est suffisamment démontrée. La puissance d'un état existe essentiellement au sein de la perception de sa puissance. Un engagement démontré et approfondi envers le développement des efforts de cybersécurité sur le continent est donc requis. La prospérité future de l'Afrique et la sécurité de son peuple en dépendent. » □

LA COLLABORATION DANS UNE GUERRE SANS FRONTIÈRE



LES FORCES DE SÉCURITÉ
AFRICAINES DOIVENT TRAVAILLER
ENSEMBLE POUR RÉPONDRE
AUX MENACES ÉMERGENTES



Le Dr Jabu Mtsweni est directeur du Centre d'information et de recherche en cybersécurité au Conseil pour la recherche scientifique et industrielle (CSIR) de Pretoria (Afrique du Sud). Il s'est entretenu avec ADF sur les types de cyber-menaces que les pays africains affrontent et la façon dont ils pourraient mieux se préparer pour les gérer. Ses commentaires ont été modifiés pour les adapter à ce format.

ADF : Pourriez-vous fournir quelques informations sur vos antécédents en matière de cybersécurité, notamment vos études et votre formation.

Dr Mtsweni : Mes antécédents concernent la science informatique ; mes qualifications de premier cycle aussi bien que mon doctorat et mes études postuniversitaires relèvent de l'informatique, sans pour autant se concentrer initialement sur la cybersécurité. J'ai commencé à être concerné par la cybersécurité, ou à m'y spécialiser, vers 2014. Mais je travaille sur divers aspects de la cybersécurité de façon limitée depuis 2003 environ. J'ai participé à un certain nombre d'initiatives, telles que la direction d'un groupe de chercheurs (au nombre de quinze environ), fortement axées sur le soutien des forces armées dans les domaines de la guerre cybernétique et du développement des capacités. Aujourd'hui, je soutiens une équipe beaucoup plus nombreuse d'environ soixante-dix personnes. Nous nous concentrons sur le soutien au département de la Défense d'Afrique du Sud et d'autres pays, mais nous abordons les questions de cybersécurité de façon générale, dans le secteur public aussi bien que dans le privé.

ADF : Veuillez expliquer brièvement ce que fait le CSIR et quelle est votre fonction en tant que directeur du Centre d'information et de recherche en cybersécurité du CSIR.

Dr Mtsweni : Le CSIR est une entreprise nationale d'état qui est uniquement axée sur la recherche et le développement au sein de divers secteurs socioéconomiques : par exemple l'eau, l'énergie, l'environnement, la santé, les questions relatives à la sûreté et la sécurité, à la logistique, aux lieux intelligents, aux TIC [technologies de l'information et de la communication]. Mon domaine particulier de spécialisation est évidemment celui de la défense et la sécurité. Je dirige le Centre d'information et de recherche en cybersécurité où nous sommes principalement axés sur la recherche et l'innovation concernant les nouveaux moyens de nous protéger et de protéger nos organisations et nos forces armées, ainsi que développer certaines technologies sous forme de prototypes, puis de commercialiser quelques-unes de nos PI [propriétés intellectuelles] locales.

ADF : Quelle est la menace de cybersécurité la plus grande et la plus prédominante qui pèse sur le continent africain et comment les pays devraient-ils riposter ?

Dr Mtsweni : Je pense que la plus grande menace est évidemment celle qui pèse sur la souveraineté des pays du point de vue de l'espace numérique. Autrement dit,

lorsque la souveraineté de l'espace numérique des pays est compromise, que ce soit par des fuites de données, par des problèmes de logiciel de rançon ou par le vol de la PI, de la propriété intellectuelle ou des informations sensibles des pays d'Afrique. Cette menace est importante parce que, en géopolitique, c'est aussi une question d'influence : différents pays peuvent souhaiter influencer la politique ou toute autre chose en Afrique. La question des données ou de l'information volées ou compromises devient donc la plus grande menace qui pèse en Afrique.

L'activité ou l'action clé que les forces armées africaines doivent suivre concerne le développement des capacités du cyberspace. Et lorsque nous parlons de développer ces capacités, nous n'évoquons pas seulement la technologie, nous n'évoquons pas seulement les données. Nous parlons en fait de la gamme complète, de la capacité des gens à comprendre le domaine cybernétique : c'est exactement comme la fourniture d'une formation pour que les gens puissent protéger l'espace aérien, terrestre ou maritime. Nous devons promouvoir la capacité de responsabiliser nos forces ou de leur enseigner à bien comprendre l'univers cybernétique.

Nous devons aussi mettre en place des processus du point de vue politique et posséder des stratégies qui vont répondre de façon proactive à certaines de ces menaces. Nous devons bien comprendre nos données. Les pays doivent bien comprendre ce qu'ils protègent, parce qu'il est très difficile de protéger ce que vous ne comprenez pas. Si vous comparez cela à la protection terrestre, aérienne ou peut-être maritime, il est très facile d'identifier les atouts que vous protégez, mais dans le cyberspace le domaine est un peu plus vaste et donc la portée est un peu plus vaste. Nous avons donc besoin de plus de sensibilisation, mais aussi de plus en plus de formation. Et bien entendu nous avons besoin des ressources et des outils qui pourraient nous aider à nous protéger nous-mêmes et à pouvoir détecter les menaces au moment où elles se manifestent dans le cyberspace.

ADF : Quelles sont les façons, le cas échéant, dont le CSIR ou ses divisions conseillent et assistent la Force nationale de défense d'Afrique du Sud sur le type de questions de cybersécurité que vous venez d'évoquer ?

Dr Mtsweni : Le CSIR est ce que nous appelons un conseiller indépendant d'acheteur ou d'utilisateur intelligent pour un certain nombre d'agences gouvernementales. Au sein de l'espace militaire, et en particulier de la guerre de l'information et la guerre cybernétique, nous jouons un rôle tout

à fait crucial. Ceci inclut par exemple la construction de prototypes pour les forces armées, afin de pouvoir mieux comprendre comment certaines capacités peuvent être mises à disposition pour les utiliser dans un environnement réel. Nous conduisons beaucoup de recherche et de développement pour elles, afin qu'elles puissent comprendre le panorama de la menace. Nous faisons aussi beaucoup de travail afin de les conseiller sur certaines des technologies qu'elles devraient utiliser, ou qu'elles ne devraient pas utiliser, sur la façon dont elles peuvent se protéger elles-mêmes contre les diverses menaces du cyberspace, et aussi, évidemment, nous les soutenons dans la construction de certaines de ces capacités afin de protéger le pays et ses citoyens.

Il existe un certain nombre d'exemples, mais une grande partie des efforts appartient au secret défense, et donc je ne peux pas vraiment parler d'un travail ou de projets spécifiques, mais je peux en parler de façon générale. En ce qui concerne la formation, nous avons soutenu les forces armées, et il y a un certain nombre d'unités qui ont été formées et habilitées grâce au CSIR pour gérer les problèmes du cyberspace. Nous avons assisté aussi les forces armées pour bien comprendre l'importance d'établir leur propre infrastructure. Et de temps à autre, nous sommes sollicités et elles nous demandent des conseils sur divers points qui affectent leur domaine d'activités.

ADF : De façon plus générale, que devraient faire les pays africains pour assurer que leur infrastructure nationale critique telle que le réseau électrique et l'alimentation en eau soit protégée contre les attaques cybernétiques ?

Dr Mtsweni : Je pense que l'une des choses cruciales que nous avons faites sur le continent, et certainement dans le domaine de la défense africaine, c'est la question de la collaboration. Je pense que, en ce qui concerne le cyberspace, les forces armées d'un pays à l'autre ne travailleraient en général pas conjointement, à moins de lutter contre un même ennemi. Mais au sein du cyberspace, je pense que la collaboration devient tout à fait cruciale. Pourquoi est-ce important ? Parce que les menaces sont presque les mêmes dans le cyberspace et lorsque nous collaborons, nous pouvons alors partager ces menaces.

Une autre chose cruciale, c'est la question de sensibilisation situationnelle. Il est difficile de protéger ce que vous ne connaissez pas ou de réagir à des incidents que vous ne constatez pas. Il est donc important pour elles de posséder cette sensibilisation situationnelle grâce à des édifices, des structures telles que nos centres nationaux de réponse aux incidents cybernétiques ou nos équipes de réponse de sécurité informatique. En plus de cela, il faut avoir de réelles politiques qui définissent ou clarifient ce que les forces armées doivent faire ou ne pas faire parce que, dans le domaine cybernétique, vous avez le côté civil, vous avez le côté de l'état-nation, et aussi le côté du secteur privé.

Donc, afin de simplement résumer dans le contexte africain : il s'agit de la collaboration, il s'agit de la sensibilisation situationnelle et il s'agit du développement

de cette capacité dont j'ai parlé ; et en plus de cela, il s'agit des structures des pays africains telles que l'Union africaine qui possède des unités de partage des renseignements sur les menaces, tout comme le fait Interpol. Je pense que les forces armées africaines pourraient avoir quelque chose comme ça, mais en plus d'une simple collaboration propre, nous devons aussi collaborer avec d'autres nations en Europe, avec les États-Unis, parce que je pense qu'il est important pour nous d'avoir des alliés et des partenaires.

ADF : Quelques pays ont créé un commandement cybernétique ou mis l'accent sur une formation cybernétique au sein de leurs forces armées. Pensez-vous que la cybersécurité doit être l'objet d'un focus plus important chez les forces armées africaines ? Plus particulièrement, que devraient faire les forces armées dans ce sens ?

Dr Mtsweni : Je pense que l'accent mis sur la cybersécurité est très important, et je pense qu'elle est accentuée et rendue importante par le fait que nous avons déjà constaté un grand nombre d'attaques contre les états-nations. Et nous avons déjà constaté beaucoup de violations en Afrique qui sont présumées provenir de pays étrangers. Même en Afrique du Sud, nous avons perdu des propriétés intellectuelles, par exemple la conception d'un avion militaire, du fait des attaques cybernétiques. Il est donc très important de disposer de ces capacités, non seulement sous forme documentaire, mais aussi sous forme opérationnelle, y compris la formation du personnel. Il existe quelques pays qui ont une défense cybernétique robuste ; par défense, je veux dire offensive et défensive. Nous avons donc besoin d'y arriver, parce qu'il s'agit aussi de développer nos propres outils ; si vous considérez les États-Unis, ils ont leur propre commandement cybernétique mais ils effectuent continuellement du R&D [recherche et développement], en construisant leurs propres outils pour la défense et pour l'attaque lorsque cela est nécessaire.

ADF : Nous avons beaucoup parlé de la formation de façon générale, mais il y a aussi la formation au micro-niveau, c'est-à-dire au niveau du soldat individuel. Pour cela, quelle formation ou quels principes devraient être intégrés dans la formation de toutes les forces militaires et de sécurité pour assurer qu'elles aient une compréhension de base des pratiques importantes et efficaces de cybersécurité ?

Dr Mtsweni : Je pense que la formation générique concerne évidemment la compréhension des réseaux, parce que si vous ne comprenez pas la technologie il sera très difficile pour vous de la protéger ou de l'attaquer. Et la deuxième chose consiste à les former sur la sensibilisation de base en cybersécurité. Parce que si quelqu'un n'est pas sensibilisé sur ce qui menace les outils qu'il utilise, ceci pourrait être un problème. Donc, tout simplement les principes de base, l'emploi des réseaux sociaux par les forces militaires, l'emploi de ces différentes technologies et des dispositifs mobiles, ainsi de suite, parce que lorsqu'ils sont sensibilisés, ils peuvent bien comprendre ce que sont les menaces et comment ces menaces peuvent être mises à l'échelle.

Transnet, société d'état sud-africaine de transport et de logistique, a été frappée par une attaque cybernétique en juillet 2021. L'attaque a duré plusieurs jours. AFP/GETTY IMAGES



ADF : Les attaques cybernétiques soutenues par les états sont aujourd'hui une réalité en Afrique. Nous avons constaté au cours des années récentes les agences gouvernementales qui étaient frappées par un logiciel de rançon et les entreprises privées frappées par un piratage soutenu depuis l'étranger. Dans quelle mesure êtes-vous préoccupé par les états qui emploient ces attaques cybernétiques comme outil de guerre, et pensez-vous que cet emploi augmentera en Afrique au cours des prochaines années ?

Dr Mtsweni : Les attaques cybernétiques employées comme outils de guerre entre nations augmentent, elles sont en hausse. Et parfois c'est seulement une nation qui les utilise, simplement des partis politiques qui s'attaquent en utilisant certains de ces outils. Et nous constatons définitivement cela de plus en plus en Afrique. Nous le constatons maintenant en particulier sur les réseaux sociaux, et maintes fois pour l'accès à la technologie.

En ce qui concerne ce point, je voulais souligner que la cybersécurité est une question de pouvoir. Ceux qui ont les outils, ceux qui ont le personnel, ceux qui ont la capacité sont capables de conduire certaines de ces attaques. Puis vous avez ceux qui n'ont pas [ces capacités] dans le domaine de la cybersécurité : ceux-ci sont impuissants, ils pourraient être incapables d'y répondre. Il est donc important que les pays africains se préparent pour des capacités de défense cybernétique holistiques et totales.

ADF : Les groupes extrémistes utilisent le web depuis des années pour le recrutement et la propagation de la propagande ; existe-t-il des preuves quelconques que les groupes extrémistes essaient d'utiliser des capacités cybernétiques pour lancer des attaques telles que le logiciel de rançon ou d'autres types d'attaque sur le continent africain ? Les pays devraient-ils en être préoccupés ?

Dr Mtsweni : Je pense qu'en Afrique l'emploi des outils de guerre cybernétique par les groupes extrémistes est limité, mais il y a des exemples, même s'ils sont rares et sporadiques. En ce qui concerne le logiciel de rançon, je ne possède pas beaucoup de preuves, mais nous avons constaté que des groupes extrémistes... ciblaient les gouvernements, et en Afrique du Sud nous l'avons beaucoup constaté. Par exemple, le département de la Justice a été attaqué et Transnet a aussi été sujet au piratage par

un logiciel de rançon. Nous pourrions ne pas connaître certains de ces événements parce qu'ils ne vont pas nécessairement en parler mais nous examinons cela attentivement et nous le constatons.

ADF : En ce qui concerne les groupes extrémistes tels que Boko Haram et al-Shebab, voyez-vous des indications quelconques que ce genre de groupe fasse plus que simplement recruter sur le web et qu'il utilise des capacités cybernétiques à des fins militaires pour atteindre ses objectifs djihadistes, extrémistes ou politiques ?

Dr Mtsweni : Je pense qu'il existe définitivement des preuves de cela, bien qu'elles soient limitées. Mais considérons simplement l'exemple typique des réseaux sociaux. Si vous considérez les réseaux sociaux comme un outil cybernétique... il pourrait être utilisé par ces groupes extrémistes, et nous constatons qu'ils emploient vos deep-fakes, vos réseaux sociaux pour propager des informations fallacieuses. Parce que dans notre contexte, le problème de la propagation des informations fallacieuses est aussi une autre façon de conduire des opérations psychologiques si vous examinez le point de vue psychique, parce qu'il s'agit d'influencer les gens, il s'agit de diffuser la propagande, il s'agit de changer le récit. Et nous constatons que l'emploi des réseaux sociaux sous forme d'attaque numérique est en hausse en Afrique.

En ce qui concerne leur emploi des outils cybernétiques durs, il n'existe pas beaucoup de preuves, mais pour l'attaque des communications et pour les opérations psychologiques, nous constatons qu'ils sont très performants, en particulier pour promouvoir ces différentes théories du complot.

ADF : Souhaiteriez-vous mentionner quelque chose d'autre en plus des réponses à mes questions ?

Dr Mtsweni : Le cyberterrorisme a définitivement un impact sur la sécurité humaine et je pense que les forces armées, y compris les agences de mise en application de la loi, ont un grand rôle à jouer alors que l'emploi du numérique est en hausse. Il est important de développer des capacités et de nous préparer. La question n'est pas de savoir si cela va se produire, c'est de savoir quand cela se produira. □

LE CAP

OUBLIÉ



LA GÉOGRAPHIE. L'HISTOIRE. LA POLITIQUE. LES ERREURS. TOUT CELA JOUE UN RÔLE DANS LA MONTÉE DE L'EXTRÉMISME VIOLENT DANS LA PROVINCE MOZAMBICAINE DU CABO DELGADO.

PERSONNEL D'ADF

PHOTOS PAR : AFP/GETTY IMAGES

Alors que de jeunes hommes rôdaient dans les rues de Mocímboa da Praia avec des machettes et des AK-47 le 5 octobre 2017, certains habitants regardaient attentivement par la fenêtre. Ils avaient peur et filmaient la marche défiante sur leur téléphone cellulaire.

Au moment où un militant brandissant un fusil passe à côté, un résident murmure ce nom infâme et terrifiant : « al-Shebab ».

Cette scène fait partie d'un documentaire de BBC Africa Eye intitulé : « Les fils de Mocímboa : la crise du terrorisme au Mozambique », qui décrit les défis lancés par le groupe terroriste qui tourmente la province du Cabo Delgado depuis cette première attaque remontant à octobre 2017. Dans cet assaut, environ trente insurgés ont assiégé les trois postes de police de la municipalité ; tué dix-sept personnes, y compris deux policiers ; et attaqué les armureries. Le Cabo Delgado est connu par le sobriquet de Cabo Esquecido, qui signifie le « Cap oublié ».

Les habitants locaux se servent du nom d'al-Shebab, qui veut dire « les jeunes », de façon informelle pour se référer au groupe. Mais il n'est pas affilié au groupe terroriste du même nom lié à al-Qaïda en Somalie. Il est aussi appelé Ansar al-Sunna, ce qui signifie « sympathisants de la tradition ».

L'attaque de 2017 était la première de toute une série dans la région, ayant conduit à la mort d'un total de plus de 3.700 personnes et au déplacement de plus de 850.000 en date de février 2022. Les soldats et les policiers rwandais sont entrés dans le pays en juillet 2021 et ont bientôt reconquis Mocímboa da Praia avec des effectifs de 1.000 soldats.

La mission multinationale de la Communauté de développement d'Afrique australe au Mozambique (SAMIM) a été déployée quelques jours après les forces rwandaises, ce qui a ajouté plusieurs centaines de soldats aux troupes du Mozambique. Ces soldats provenaient des huit pays participants : Afrique du Sud, Angola, Botswana, Lesotho, Malawi, République démocratique du Congo, Tanzanie et Zambie. Les troupes terrestres provenaient principalement de l'Afrique du Sud, du Botswana, du Lesotho et de la Tanzanie alors que les autres participants ont contribué un soutien logistique, selon le reportage du quotidien sud-africain Daily Maverick en janvier 2022.



Les policiers rwandais (à gauche) et les soldats mozambicains se tiennent au garde-à-vous lors d'un événement le 24 septembre 2021 à Pemba (Cabo Delgado).

Alors même que les forces mozambicaines, rwandaises et de la SAMIM enregistrèrent des succès notables pendant le deuxième semestre 2021 et au début 2022, la violence brutale a persisté et, avec elle, des questions se sont posées pour déterminer si l'insurrection aurait pu être éliminée plusieurs années auparavant.

DES ANTÉCÉDENTS D'ISOLEMENT

La municipalité portuaire de Mocímboa da Praia est située à plus de 2.600 km de route de Maputo, la capitale du Mozambique. La grande distance avec les centres gouvernementaux est une caractéristique fréquente des zones radicalisées dans les pays africains. Ces distances ont tendance à conduire à la réduction de la présence et des services du gouvernement dans les zones reculées, ce qui suscite une perception de marginalisation de la part des habitants locaux. Des exemples incluent le Nord du Mali, origine de l'extrémisme djihadiste métastasé dans le pays, et le Nord du Nigeria, foyer de l'insurrection de Boko Haram.

La distance est encore plus exacerbée par le fait que le Mozambique est toujours en cours de rétablissement après une guerre civile brutale qui a duré de 1977 à 1992. On estime que la guerre a tué un million de personnes et déplacé des millions de plus. En outre, la côte du Cabo Delgado est en général associée au mouvement rebelle



Un soldat rwandais conduit une patrouille près d'un camion incendié à Palma (Cabo Delgado) en septembre 2021.

Ce camp pour déplacés internes dans le district de Metuge du Cabo Delgado abritait environ 30.000 personnes en mai 2021, une fraction de toutes les personnes déplacées par l'insurrection.

de la Résistance nationale du Mozambique, connu sous le nom de RENAMO. Au cours de la guerre, ses forces ont lutté contre le Front de libération du Mozambique, appelé FRELIMO, qui est aujourd'hui dirigé par le président mozambicain Filipe Nyusi.

Certains déclarent que cette division politique sert à séparer davantage le Cabo Delgado et son peuple de l'attention et de la préoccupation du gouvernement. Une autre question régionale majeure concerne la découverte et la capitalisation de vastes ressources de gaz naturel, et de mines de rubis de plus petite envergure. Les experts notent que les habitants locaux sont exclus, et parfois éloignés, des sites de mines de rubis dans la région après avoir bénéficié de leur commerce artisanal pendant plusieurs années, perdant ainsi l'accès aux opportunités économiques, y compris celles qui sont illicites.

La géographie, l'histoire et la politique : elles peuvent toutes être blâmées à des degrés variables pour les conditions actuelles au Cabo Delgado. Mais les experts disent que le gouvernement du Mozambique a aussi commis des erreurs dans le passé, en manquant de respecter les avertissements et les craintes émergentes de la communauté. Si les forces de sécurité avaient déjà fait attention en 2015, peut-être que l'insurrection aurait pu être efficacement confrontée dans sa phase précoce.

LA RÉPONSE DU MOZAMBIQUE

Après la fin de l'assaut d'octobre 2017, la police mozambicaine est arrivée. Elle a accusé des bandits d'avoir commis la violence et elle a déclaré qu'elle solutionnerait le problème en une semaine, a déclaré à ADF le Dr Salvador Forquilha, chercheur principal à l'Institut des études sociales et économiques du Mozambique.

Il a dit que le gouvernement avait commis plusieurs erreurs graves en 2017. Premièrement, les responsables de la sécurité ont répondu par la violence, ils ont fermé



les mosquées et ils ont procédé rapidement à quelques arrestations. Ceci a semé la confusion et a aussi provoqué un émoi parmi les Musulmans mozambicains, selon des reportages.

« Je pense que le gouvernement n'était pas prêt à contrôler un tel phénomène, déclare le Dr Forquilha à ADF. Souvenez-vous que la guerre civile avait duré seize ans et que nous sommes toujours en train de clôturer le processus de la guerre civile avec la réintégration des ex-guérilleros du groupe rebelle RENAMO. ... Ceci a donc été une surprise. »

Finalement, dit-il, il existait des problèmes d'organisation et de coordination entre la police et les forces armées. Parfois, ce manque de coordination a conduit à des conflits entre les deux groupes. À mesure que ce problème persistait, les insurgés ont avancé de plus en plus jusqu'à ce que les forces rwandaises et de la SAMIM soient déployées en 2021.

« Je pense que l'approche du gouvernement visant à contrôler le phénomène était incorrecte dès le début, et le gouvernement a réalisé vraiment tard que le pays affrontait un problème sérieux lié au djihadisme et au terrorisme », a dit le Dr Forquilha à ADF.

L'ORIGINE DE L'EXTRÉMISME

L'assaut d'octobre 2017 est généralement considéré comme la première attaque organisée et coordonnée d'Ansar al-Sunna. Mais ce n'est pas le premier épisode de violence au Cabo Delgado, ni la première indication des enseignements islamiques radicaux sévissant dans la région.



Une femme porte un enfant parmi les ruines d'un village incendié par les insurgés à l'extérieur de Macomia dans la province mozambicaine du Cabo Delgado.

**« JE NE PENSE PAS
QU'UN SEUL PAYS
PUISSE COMBATTRE
LE TERRORISME, LE
DJIHADISME, QUOI QUE
CE SOIT D'AUTRE, SANS
COOPÉRER AVEC D'AUTRES
PAYS, D'AUTRES ÉTATS,
D'AUTRES NATIONS. »**

— **Dr Salvador Forquilha**
Chercheur principal à l'Institut des
études sociales et économiques



Ansar-al-Sunna est apparu en 2015 en attaquant les Musulmans locaux. Le documentaire de BBC Eye montre que les chefs locaux sonnaient l'alarme d'une nouvelle forme d'instruction islamique qui s'infiltrait dans la région en 2015.

Le maire de Mocímboa da Praia avait annoncé qu'un groupe appelé al-Shebab recrutait les jeunes dans la région, ce qui constituait une menace pour la paix, selon le reportage de BBC Eye. Un an plus tard en 2016, un directeur d'école déclarait à la station radio communautaire Nacedje de Macomia que l'absentéisme augmentait dans son école. Il en accusait une secte islamique qui affirmait qu'il était inutile d'aller à l'école.

Un chef local a envoyé en 2016 au conseil musulman local une liste de préoccupations qui énumérait des éléments étranges de sermon de la part des insurgés. Ces instructions disaient aux fidèles de prier sans se déchausser, de ne pas porter de pièce d'identité et d'éviter les écoles d'état, le drapeau national et les événements nationaux. « Ils ont recruté des Musulmans qui sont ignorants, qui n'ont pas étudié et qui sont pauvres », a-t-il dit dans le reportage de la BBC.

Le Dr Forquilha a déclaré à la BBC : « Les chefs musulmans donnaient en fait des avertissements, et certains d'entre eux se sont réunis avec les responsables locaux en disant qu'ils faisaient face à de nombreux défis dans les mosquées locales, et qu'ils voyaient des gens venant de l'étranger, en particulier des jeunes, qui essayaient de prêcher un Islam très radical. Il n'y a pas eu de mesures très claires de la part du gouvernement... dans le but de lutter contre le groupe dès le début. »

DES INFLUENCES ÉTRANGÈRES

Les problèmes liés à l'incompétence gouvernementale existent depuis longtemps dans la province du Cabo Delgado et les régions voisines. Mais les racines de l'Islam radical peuvent provenir de l'extérieur de cette zone, de l'autre côté de la frontière tanzanienne et d'ailleurs, selon certains experts. Le Centre africain pour les études stratégiques (ACSS) a conduit un webinaire en octobre 2021 sur les origines de la violence au Cabo Delgado.

Dino Mahtani, directeur adjoint du Programme Afrique de l'International Crisis Group à l'époque, y a remarqué que la répression des radicaux islamiques en Tanzanie en 2017 aurait pu pousser les extrémistes vers le Mozambique, où ils se seraient associés aux extrémistes locaux.

Cette répression, selon M. Mahtani, a ciblé ceux qui étaient affiliés « aux franchises d'al-Qaïda sur la côte de Zanguebar » entre la Somalie, le Kenya, la Tanzanie et le Mozambique. Il dit que l'État islamique essaie de « percer » le réseau et de le placer sous son influence, ce qui s'est déjà produit avec les Forces démocratiques alliées de la République démocratique du Congo. Des recherches montrent que des Tanzaniens recrutés depuis 2017 se trouvaient dans des camps à l'Est de la RDC, puis sont venus au Cabo Delgado. « Il y a donc

des va-et-vient des jeunes de la côte de Zanguebar qui participent aux conflits violents, non seulement au Cabo Delgado mais aussi dans l'Est du Congo », selon M. Mahtani.

Le Dr Adriano Alfredo Nuvunga, directeur du Centre pour la démocratie et le développement, organisation de la société civile sans but lucratif du Mozambique, convient que des influences externes ont façonné l'insurrection du Cabo Delgado.

Cette région, déclare-t-il dans le webinaire de l'ACSS, est marginalisée et négligée depuis longtemps par le gouvernement central. « L'ensemble du tissu social qui favorise les conflits est lié aux problèmes locaux », dit-il par l'intermédiaire d'un interprète. Mais la violence barbare commise par les insurgés, qui emploie des décapitations et des amputations de membre, indique des méthodes terroristes exportées au Cabo Delgado depuis l'étranger.

QU'AURAIT-ON PU FAIRE ?

Le Dr Forquilha est d'accord sur ce point : beaucoup d'extrémistes proviennent de Tanzanie. « Ce qui est surprenant, c'est par exemple de constater que le gouvernement a mis si longtemps pour coopérer avec la Tanzanie », a-t-il dit à ADF. Le Mozambique aurait pu mieux savoir à quoi s'attendre et apprendre comment gérer l'insurrection en s'engageant avec le Kenya, l'Ouganda et la Tanzanie : chacun de ces pays confronte depuis des années la violence extrémiste.

Les autres pays africains affrontant des défis similaires feraient bien de prendre au sérieux les menaces potentielles dès le début, dit-il. Ceci inclut l'emploi efficace des services de renseignement d'état et les mesures essayant d'assurer que les institutions gouvernementales sont suffisamment robustes pour fournir une résilience et des opportunités économiques aux résidents.

Si le gouvernement mozambicain avait suivi cette approche plus collaborative dès le début, déclare le Dr Forquilha, il aurait pu empêcher les insurgés de s'ancrer inextricablement dans toute la région, ce qui a conduit à un grand nombre de déplacés internes et à d'autres problèmes.

Le Dr Forquilha, qui a conduit des études et des recherches dans les zones affectées du Cabo Delgado, se trouvait dans la région en janvier 2022. Il a parlé aux résidents de Pemba, municipalité portuaire et capitale de la province. Les résidents lui ont dit qu'ils « sont toujours attaqués dans certains lieux » malgré la présence des forces militaires multinationales. De petits groupes d'insurgés ciblent maintenant les petits villages pour les attaquer. Pour les soldats, ceci sera plus difficile et plus long à combattre. Les forces militaires peuvent améliorer le secteur de la sécurité « mais elles n'élimineront pas l'insurrection elle-même », dit-il.

Avant l'intervention des forces rwandaises et de la SAMIM, le Mozambique s'était tourné vers des sociétés militaires privées, d'abord l'infâme groupe Wagner de Russie et ensuite le groupe Dyck Advisory basé en



Un soldat rwandais faisant partie des effectifs de 1.000 soldats et policiers conduit une patrouille près de Palma (Cabo Delgado) en septembre 2021.

Afrique du Sud. Les forces de Wagner sont parties après avoir subi de lourdes pertes et Dyck est parti à l'expiration de son contrat au début 2021. Les participants au webinaire de l'ACSS conviennent avec le Dr Forquilha qu'il est improbable qu'une intervention militaire à elle seule puisse mettre fin à l'insurrection au Mozambique.

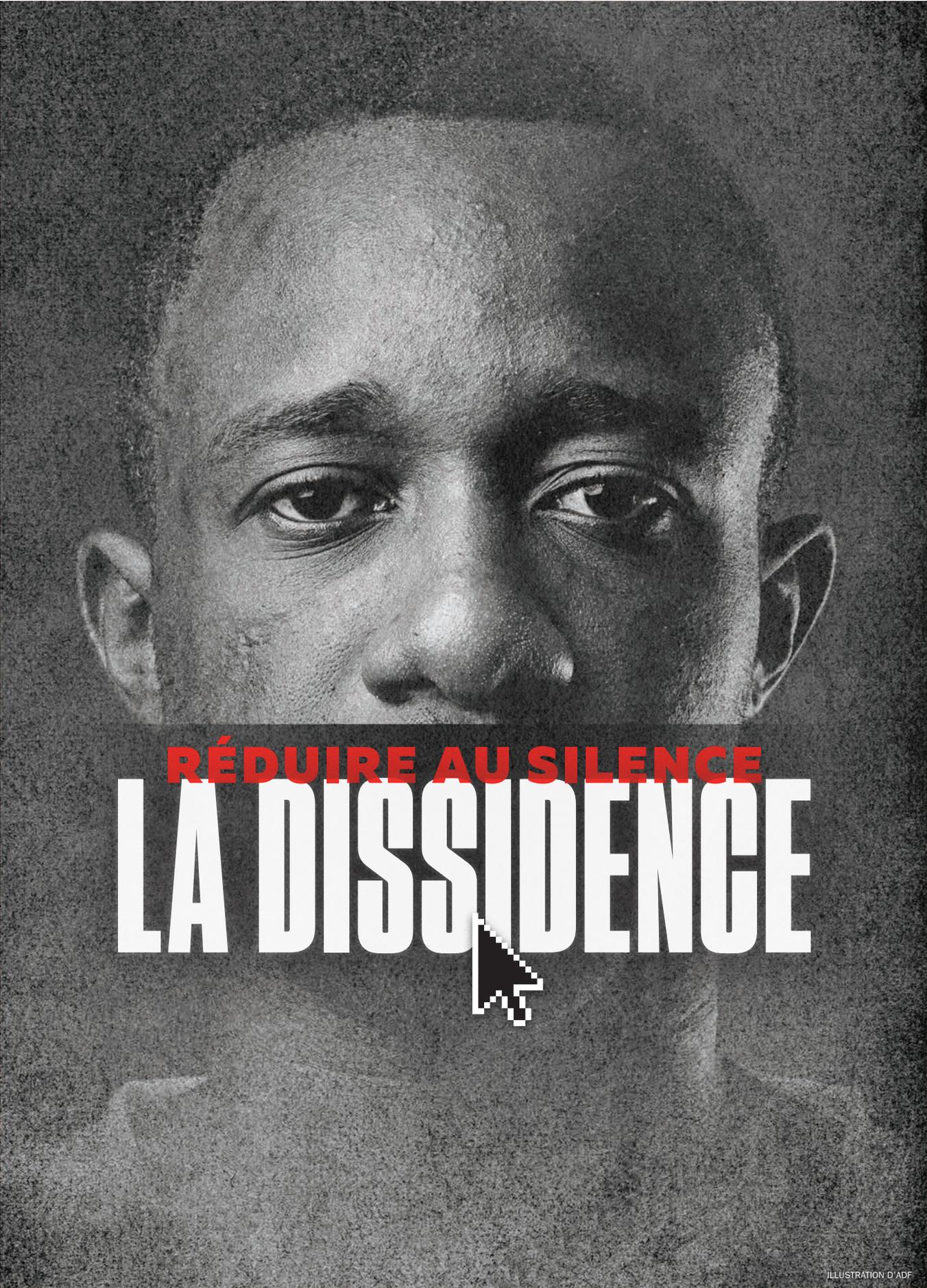
Idriss M. Lallali, directeur de l'unité d'alerte et de prévention au Centre africain d'étude et de recherche sur le terrorisme, a comparé la situation au Mozambique avec ce qui se passe au Mali depuis 2012. Le Mozambique doit « restaurer la présence de l'état » et développer la confiance entre l'état, le secteur de la sécurité et le peuple qu'ils servent.

« Si vous ne développez pas certaines régions de votre pays, elles tomberont et reviendront pour vous hanter à un moment ou à un autre, a dit M. Lallali dans le webinaire. Et je pense que ce qui s'est passé au Mali se passe maintenant au Mozambique. »

À ce moment, déclare le Dr Forquilha, le Mozambique devra apporter une dynamique interne aux efforts socio-économiques visant à adresser la pauvreté et le manque d'emplois. Ceci contribuerait beaucoup à donner aux jeunes des opportunités autres que le recrutement par les extrémistes. De tels efforts doivent aussi atteindre les provinces voisines de Nampula, Niassa et la Zambézie, où les conditions sont similaires.

La dimension externe des liens d'Ansar al-Sunna avec les organisations terroristes internationales telles que l'État islamique et les réseaux d'Afrique de l'Est souligne le besoin de coopération avec les autres pays. L'État islamique a commencé à revendiquer des attaques d'insurgés en 2019, « donc le lien existe et nous ne pouvons pas le nier », déclare le Dr Forquilha.

« Je ne pense pas qu'un seul pays puisse combattre le terrorisme, le djihadisme, quoi que ce soit d'autre, sans coopérer avec d'autres pays, d'autres états, d'autres nations, déclare le Dr Forquilha. Parce que cela est devenu une sorte de phénomène mondial, une menace mondiale, et il doit être traité comme tel. Il est donc tout à fait important de prendre en compte la composante de la coopération. » □



RÉDUIRE AU SILENCE
LA DISSIDENCE

ILLUSTRATION D'ADF



LES FERMETURES, LA LÉGISLATION ET L'INFLUENCE ÉTRANGÈRE FONT PARTIE D'UN EFFORT POUR CENSURER L'EXPRESSION

PERSONNEL D'ADF
PHOTOS PAR : AFP/GETTY IMAGES

Lorsque Twitter supprima un message du président nigérian Muhammadu Buhari en 2021, le Nigeria interdit pendant sept mois l'accès au site de réseaux sociaux le plus populaire du pays.

Le blogueur nigérian et expert en réseaux sociaux J.J. Omojuwa a déclaré à ADF : « La perte a été gigantesque. On s'est rendu compte que ceci pouvait arriver n'importe où. »

NetBlocks, analyste de l'Internet, estime que la censure a fait perdre aux Nigériens jusqu'à 1,6 milliard de dollars sous forme d'affaires manquées. Elle a aussi perturbé les informations vitales sur le Covid-19 que le Centre pour le contrôle des maladies du Nigeria publiait sur la plateforme. Les groupes défenseurs des droits humains ont condamné la censure comme une violation de la liberté d'expression des Nigériens. En fin de compte, le gouvernement restaura l'accès, mais seulement lorsque Twitter accepta de payer des impôts et d'établir un bureau local sujet aux lois du Nigeria.

La censure nigériane de Twitter s'inscrit dans le cadre d'une série d'actions directes et indirectes conçues pour contrôler comment l'information est diffusée. Et ces censures d'information deviennent plus fréquentes en Afrique. Dans bien des cas, les contrôles sont imposés au nom de la sécurité nationale. Mais les perturbations qui en résultent diminuent la sécurité en paralysant les économies locales, interrompant l'éducation et encourageant la désinformation.

En plus des censures de l'Internet, les efforts en Afrique incluent les nouvelles lois ciblant la cybercriminalité et les campagnes menées par les forces chinoises et russes pour façonner l'environnement médiatique africain. Dans l'ensemble, ils constituent une tentative à grande échelle pour contrôler le flux de l'information sur le continent.

« En ce qui concerne la liberté d'expression, il faut toujours la défendre », déclare M. Omojuwa.

LES FERMETURES DE L'INTERNET

L'instrument le plus direct que les responsables emploient pour censurer les citoyens est la fermeture de l'Internet. L'Afrique est au premier rang mondial de ces fermetures selon Surfshark, société de surveillance de l'Internet. Depuis 2015, 32 pays africains ont pris cette mesure pour

limiter le flux d'information sur leur territoire. Entre septembre 2020 et janvier 2022, les pays africains ont été responsables pour la moitié des 24 perturbations de l'Internet dans le monde.

À lui seul, le Burkina Faso a coupé l'accès à l'Internet trois fois entre novembre 2021 et janvier 2022, y compris pendant le coup d'état qui a renversé le président Roch Marc Christian Kaboré.

Les coups d'état, les manifestations contre le gouvernement et les élections sont les événements qui provoqueront le plus probablement une censure complète ou partielle. En Algérie et en Éthiopie, les responsables ont bloqué l'accès à Internet en 2021 pour empêcher la fraude pendant les examens scolaires nationaux. L'Éthiopie a aussi imposé une censure médiatique pour contrôler les actualités liées à la guerre civile en cours dans la région du Tigré.

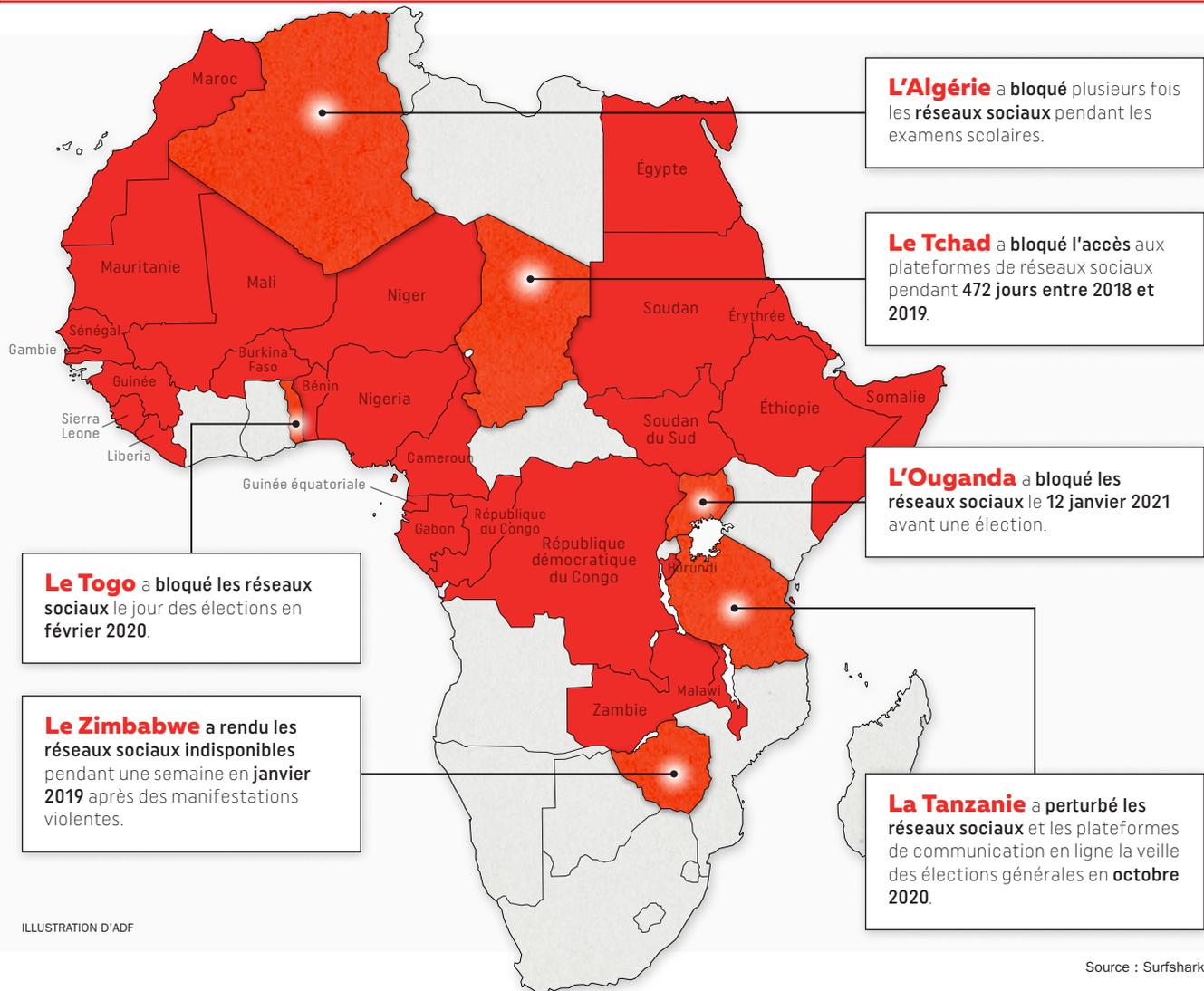


Des Nigériens manifestent contre la fermeture de Twitter par le gouvernement en juin 2021, après la suppression par le site médiatique d'un message du président Muhammadu Buhari, qui enfreignait selon elle ses conditions de service.

Dans certains cas, les responsables ont le vif souhait de supprimer l'utilisation des réseaux sociaux. Il existe une raison évidente pour cela, selon Lawrence Muthoga, ancien directeur de l'engagement communautaire pour Microsoft 4Afrika basée au Kenya.

M. Muthoga a déclaré lors d'une discussion sur la censure africaine parrainée par le groupe kényan Moringa sur Twitter Spaces : « C'est parce qu'il est très facile de mobiliser les gens sur les réseaux sociaux. »

32 PAYS AFRICAINS ONT BLOQUÉ LES RÉSEAUX SOCIAUX AU COURS DES DERNIÈRES ANNÉES



« La majorité de la censure qui se produit sur le continent en ce moment-même est liée au contrôle de la mobilisation des gens ou la propagation des idées. »

M. Omojuwa pense qu'une autre force est impliquée : le fossé des générations entre les responsables africains et les jeunes citoyens doués en technologie. L'âge médian en Afrique est un peu moins de 20 ans. « Ils [les responsables] ne comprennent pas ce domaine », déclare M. Omojuwa.

La fermeture de l'Internet n'est pas aussi simple que celle d'un journal ou la réduction au silence d'un animateur radio, dit-il. Pendant la censure de Twitter au Nigeria par exemple, les Nigériens pouvaient toujours accéder à la plateforme en utilisant des réseaux privés virtuels par l'intermédiaire d'autres pays.

« C'est un domaine tellement démocratisé, dit-il. Vous ne pouvez pas empêcher les gens de parler. »

DES LIMITATIONS JURIDIQUES

Les 39 pays africains qui ont adopté des lois contre la cybercriminalité disent qu'ils ciblent la désinformation et les risques affectant la sécurité nationale. Leurs critiques

déclarent que les lois menacent le droit à la vie privée et font courir aux gens un risque d'arrestation pour exprimer leurs opinions en ligne.

Setriakor Nyomi, directeur ghanéen de la technologie pour l'école kényane Moringa (qui fournit une formation pour les emplois technologiques), a déclaré : « Les gouvernements n'ont pas vraiment compris ce que veut réellement dire la liberté d'expression dans l'ère de l'information. »

Il a dit au cours d'une conversation avec M. Muthoga sur Twitter Spaces : « Dans l'ère de l'information, la question est de savoir comment les gouvernements la gèrent. »

Les droits humains devraient guider le processus de création de la réglementation de l'Internet, selon Admiré Mare, professeur de communication, journalisme et technologie des médias à l'université des sciences de Namibie. Le Dr Mare a étudié les lois sur la cybercriminalité dans

Un homme porte une bannière contre la censure de Twitter imposée pendant sept mois par le Nigeria. Elle a provoqué des dommages de l'économie du pays estimés à 1,6 milliard de dollars.





les seize pays d'Afrique australe. Dans son rapport intitulé « Les lois sur la cybersécurité et la cybercriminalité dans la région CDA : implications sur les droits humains », il mentionne que l'Afrique du Sud est le seul pays de la région à établir une législation respectueuse des droits des citoyens.

« Dans les pays tels que la Zambie, le Zimbabwe, la Namibie et le Malawi, il existe une peur profonde selon laquelle les lois existantes ou nouvelles sont déjà utilisées à des fins de surveillance », écrit le Dr Mare dans le rapport publié avec l'Institut médiatique d'Afrique australe (MISA) du Zimbabwe.

Le projet de loi zimbabwéen sur la protection des données interdit les messages incitant à la violence contre les personnes ou les biens matériels, interdit la transmission des fausses informations conçues pour provoquer des dommages, et interdit les e-mails non sollicités, appelés couramment spam.

Le MISA déclare que la loi ne possède pas de protection pour garantir qu'elle ne sera pas utilisée pour bloquer les travaux de la société civile, punir les dénonciateurs et violer le droit constitutionnel à la liberté d'expression. Avant l'adoption du projet de loi, Transparency International Zimbabwe a déclaré qu'il entraverait la capacité du public à révéler la corruption du gouvernement.

Muchaneta Mundopa, directrice exécutive de Transparency International Zimbabwe, a écrit dans l'analyse du projet de loi par le groupe : « L'interprétation et la mise en application imprécises de la législation par les autorités sont déjà utilisées pour réprimer les citoyens qu'elles sont censées protéger. Ce projet de loi va faire empirer les choses. »

Elle cite le cas du journaliste Hopewell Chin'ono, accusé en vertu des lois précédemment en vigueur d'avoir

Les Algériennes protestent la censure gouvernementale des plaintes liées à la tentative de l'ex-président Abdelaziz Bouteflika pour obtenir un cinquième mandat en 2019. Il a démissionné la même année et il est décédé en 2021.

incité à la violence après son exposition de la corruption dans le processus d'achat des fournitures médicales liées au Covid-19 par le gouvernement. Les dénonciateurs tels que M. Chin'ono nécessitent les réseaux sociaux pour avertir le public des affaires suspectes, déclare Mme Mundopa.

« Nous considérons donc la législation proposée comme la plus récente tentative par le gouvernement de réduire au silence la société civile et les médias et de nous empêcher d'assumer notre rôle de surveillance. »

Le Nigeria a ciblé les réseaux sociaux avec deux propositions qui ont été vivement contestées par les activistes de la libre expression. En 2015, le soi-disant projet de loi sur les pétitions frivoles ciblait la désinformation en ligne et la critique des responsables publics en les menaçant d'amendes jusqu'à 10.000 dollars.

Les activistes de la liberté d'expression ont soutenu que le projet de loi aidait les responsables publics à réduire au silence leurs critiques et ont lancé la campagne #NoToSocialMediaBill sur Twitter. Face à l'opposition du public, les législateurs ont finalement rejeté le projet de loi.

Un autre projet de loi relatif aux réseaux sociaux en 2019 était conçu pour criminaliser la publication des informations fausses ou malveillantes en ligne. Ce projet de loi a aussi été finalement retiré.

M. Omojuwa déclare que les deux tentatives de limitation des communications en ligne au Nigeria ont sonné l'alarme pour les citoyens. « Quoi que fasse le gouvernement à l'avenir, il y aura toujours une opposition », dit-il.

LES MÉDIAS ET L'AUTO-CENSURE

En plus des fermetures de l'Internet et des efforts législatifs visant à réglementer l'expression en ligne, les défenseurs africains de la liberté d'expression confrontent aussi l'influence croissante des Chinois et des Russes sur l'environnement médiatique du continent.

La Chine a pendant de nombreuses années bâti un réseau continental de médias de presse et de diffusion pour promouvoir sa propre forme de journalisme pro-gouvernemental. La Chine dépense aussi beaucoup en annonces publicitaires sur certaines chaînes d'information commerciales et fournit à d'autres un équipement coûteux tel que des antennes paraboliques afin de gagner de l'influence.

La Chine parraine chaque année la formation de centaines de journalistes africains dans les salles de rédaction chinoises. Ils y apprennent la forme chinoise de journalisme, qui met l'accent sur le soutien des politiques gouvernementales plutôt que les reportages traditionnels conçus pour tenir le gouvernement responsable face aux citoyens.

« Selon les idées du régime de Pékin, les journalistes ne servent pas de contre-pouvoir ; ils servent plutôt à promouvoir la propagande des états », écrit Christophe Deloire, secrétaire général de Reporters sans frontières, dans le rapport « La poursuite chinoise d'un nouvel ordre mondial des médias ».

L'approche adoptée par la Russie est encore plus brutale. Par l'intermédiaire de son groupe Wagner, société militaire privée, elle a lancé une station de radio soutenue par des Russes en République centrafricaine (RCA) qui diffuse de la musique en plus des actualités et des talk-shows.

Valery Zakharov, conseiller russe pour la sécurité nationale du président Faustin-Archange Touadéra de la RCA, a installé deux experts russes en relations publiques dans ses bureaux pour promouvoir l'image du président.

Entre-temps, une grande partie des médias d'actualités de la RCA ont adopté une position pro-russe, en couvrant de façon exhaustive les actions russes telles que la donation d'un équipement sportif aux écoles. Sans annonce publicitaire pour soutenir leurs travaux, les journalistes de la RCA acceptent parfois de l'argent pour écrire des articles favorables aux Russes, selon l'analyste Thierry Vircoulon, coordinateur de l'Observatoire de l'Afrique centrale et australe à l'Institut français des relations internationales.

La stratégie médiatique chinoise fait partie de sa philosophie du « bateau emprunté » qui utilise les chaînes d'actualités et les journalistes africains pour publier des articles favorables à la Chine tout en encourageant une approche pro-gouvernementale.

Plus le marché médiatique est petit, plus l'influence chinoise est grande, selon Dani Madrid-Morales, professeur à l'université de Houston et expert en combines médiatiques chinoises en Afrique.

« Ce que la Chine a pu faire, c'est d'établir ces relations au niveau personnel, déclare-t-il à ADF. En créant ces liens au niveau personnel, la Chine aide à surveiller les informations publiées. »

Ceci, selon lui, crée une forme de censure plus subtile que les fermetures de l'Internet ou le contrôle législatif : c'est une autocensure par les chaînes médiatiques qui modère les reportages pour éviter de perdre le soutien financier, et des reportages favorables de la part des journalistes formés pour éviter de défier les dirigeants.

Le réseau médiatique IOL d'Afrique du Sud a été vendu récemment à un groupe dont les investisseurs sont chinois. Peu après, les rédacteurs du réseau, formés en Occident, ont été remplacés par des rédacteurs plus favorables au modèle chinois. Lorsque le chroniqueur Azad Essa a critiqué le traitement par la Chine de sa minorité ouïghour, il a perdu son emploi le jour suivant.

« Il semblerait que je sois tombé dans une fosse non négociable qui touchait le cœur même des efforts de propagande chinois en Afrique », écrit plus tard M. Essa dans Foreign Policy.



L'influence croissante de la Chine sur le panorama médiatique africain inclut la formation des journalistes africains dans les salles de rédaction basées en Chine, où l'accent est mis sur le soutien aux politiques gouvernementales.

LE FUTUR

Que sera l'avenir de la liberté d'expression au sein des communautés médiatiques et en ligne d'Afrique ? Dans l'ensemble, la tendance est orientée vers davantage de restrictions, selon Kian Vesteinsson, analyste chez Freedom House.

« Malheureusement, la liberté sur l'Internet a diminué en Afrique au cours des dernières années, écrit-il. À un haut niveau, les défis des transitions démocratiques dans les pays tels que l'Éthiopie et le Soudan ont accentué le déclin de la liberté de l'Internet dans ces pays. »

M. Omojuwa déclare que la censure de Twitter par le Nigeria s'est avérée être un échec embarrassant mais elle pourrait inspirer des imitateurs ailleurs, alors que davantage d'Africains s'expriment sur l'Internet.

« Je pense que beaucoup de gouvernements du continent examinent comment le Nigeria a imposé sa volonté à Twitter. Le Nigeria s'en est bien tiré. »

L'impact des restrictions sur la liberté d'expression sera préjudiciable à la démocratie, dit-il.

« Si les gens n'ont pas la capacité de s'exprimer, quel est l'objet de la démocratie ? » □

Parfaire les préparatifs de combat

PERSONNEL D'ADF

Ceux qui sont engagés à défendre leur pays savent qu'ils doivent aussi être prêts à aider ceux qui servent à leurs côtés. Lorsque les combats font des victimes, une action rapide peut faire la différence entre la vie et la mort. En novembre 2021, des soldats des Forces armées de Mauritanie ont travaillé avec des formateurs des forces spéciales de l'Armée de terre des États-Unis pendant la Formation d'échange combiné interarmées. Ici, un soldat mauritanien applique un garrot sur la jambe d'un camarade pendant un exercice de simulation de victime. Les soldats se sont aussi exercés à transporter les blessés en toute sécurité sur des civières dans le paysage désertique. La formation combinée a inclus d'autres aptitudes essentielles telles que les combats rapprochés, les tactiques des petites unités et la planification de mission.





SERGEANT D'ÉTAT-MAJOR NICHOLAS BYERS/
ARMÉE DE TERRE DES ÉTATS-UNIS



**Les mines terrestres
tourmentent le Zimbabwe**

40

ANNIÉES

APRÈS LA GUERRE

Ce pays d'Afrique australe espère éliminer ses mines en 2025

PAR CYRIL ZENDA

Talakufa Mudzikiti pensait que le cessez-le-feu de 1979 ayant mis fin à une guerre de 15 ans au Zimbabwe lui permettrait de chercher le bétail perdu de sa famille en toute sécurité. Mais la recherche est devenue une aventure onéreuse qu'il regrette aujourd'hui.

Alors qu'il parcourait les forêts près du village de Dumisa dans le Sud-Ouest du Zimbabwe, il a marché sur une mine antipersonnel qui lui a arraché sa jambe gauche. « Ce jour-là, ma vie a été détruite... tous mes rêves ont été ruinés », dit-il. M. Mudzikiti, aujourd'hui âgé de 70 ans, n'est pas le seul à souffrir des résultats des mines terrestres employées dans les conflits armés.

Lui-même et d'autres villageois font partie des plus de 2.000 Zimbabwéens qui ont été mutilés mais sont toujours en vie. Près de 1.700 autres ont été tués par les mines terrestres au cours des quarante dernières années.

Des zones massivement contaminées par les mines terrestres

Le Zimbabwe, appelé auparavant Rhodésie, a gagné son indépendance en 1980, après 90 ans de colonialisme et de régime de la minorité blanche. Les années 70 ont été marquées par la guerre du Bush brutale qui a tué plus de 50.000 personnes.

Pour dissuader les combattants de la libération d'entrer dans le pays depuis les états voisins du

Nombre de victimes des mines dans le monde en 2020	
Civils	4.437
Démineurs	27
Militaires	1.105
Inconnus	1.504

Source : Landmine Monitor 2021

Mozambique et de la Zambie, l'armée rhodésienne a planté un nombre de mines antipersonnel estimé à 3 millions entre 1974 et 1979 dans cinq champs de mines principaux sur 850 km le long des frontières Est et Nord du pays.

Des zones truffées de mines terrestres, certaines comportant environ 5.500 mines par km carré, sur la frontière du Zimbabwe avec le Mozambique ont entravé le développement dans les communautés marginalisées.

En date de septembre 2018, on pensait que les mines étaient réparties sur plus de 66 km carrés de terrain. Une étude de la région Nord-Est du Zimbabwe a identifié 87 communautés directement affectées par les mines, d'un total de plus de 75.000 personnes.

L'étude a aussi découvert que 78 champs de mines se trouvaient à moins de 500 mètres des zones résidentielles.

Suite à la page 35



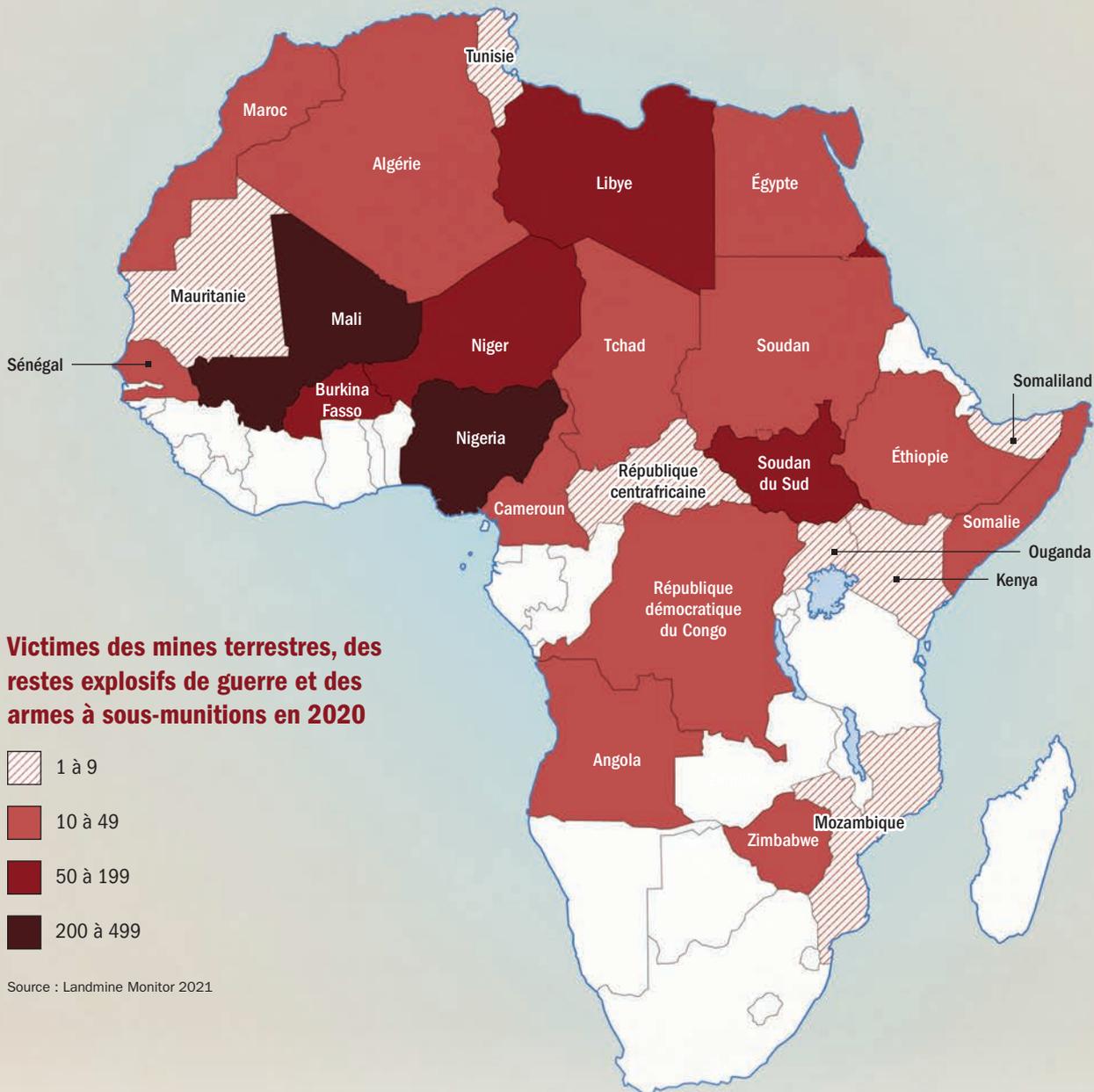
Des mines terrestres et des débris sont éliminés hors de Juba (Soudan du Sud). AFP/GETTY IMAGES



Un expert libyen du déminage montre une mine enterrée. On pense qu'elle avait été plantée par l'armée de l'ancien leader Mouammar Kadhafi près de l'aéroport international de Mitiga hors de Tripoli. AFP/GETTY IMAGES



Des victimes des mines terrestres attendent de commencer la physiothérapie au centre orthopédique Agostinho Neto de Huambo (Angola). AFP/GETTY IMAGES



Suite de la page 33

Les mines terrestres bloquent l'accès aux terrains résidentiels, entravent le commerce transfrontalier, interdisent l'accès aux terrains agricoles par les petits fermiers et affectent négativement le système sanitaire et l'élevage du bétail. De ce fait, la plupart des zones affectées ont des niveaux de pauvreté disproportionnés et des taux élevés d'insécurité alimentaire.

La stratégie nationale des mesures anti-mines

Le gouvernement du Zimbabwe, signataire de la Convention sur l'interdiction des mines antipersonnel, s'est engagé à œuvrer pour satisfaire à l'objectif d'élimination des mines terrestres en 2025 en créant l'Autorité nationale zimbabwéenne des mesures anti-mines, organisme de politique et de réglementation des mesures anti-mines dans le pays. Le Centre zimbabwéen des mesures anti-mines (ZIMAC), qui dépend de l'autorité, coordonne

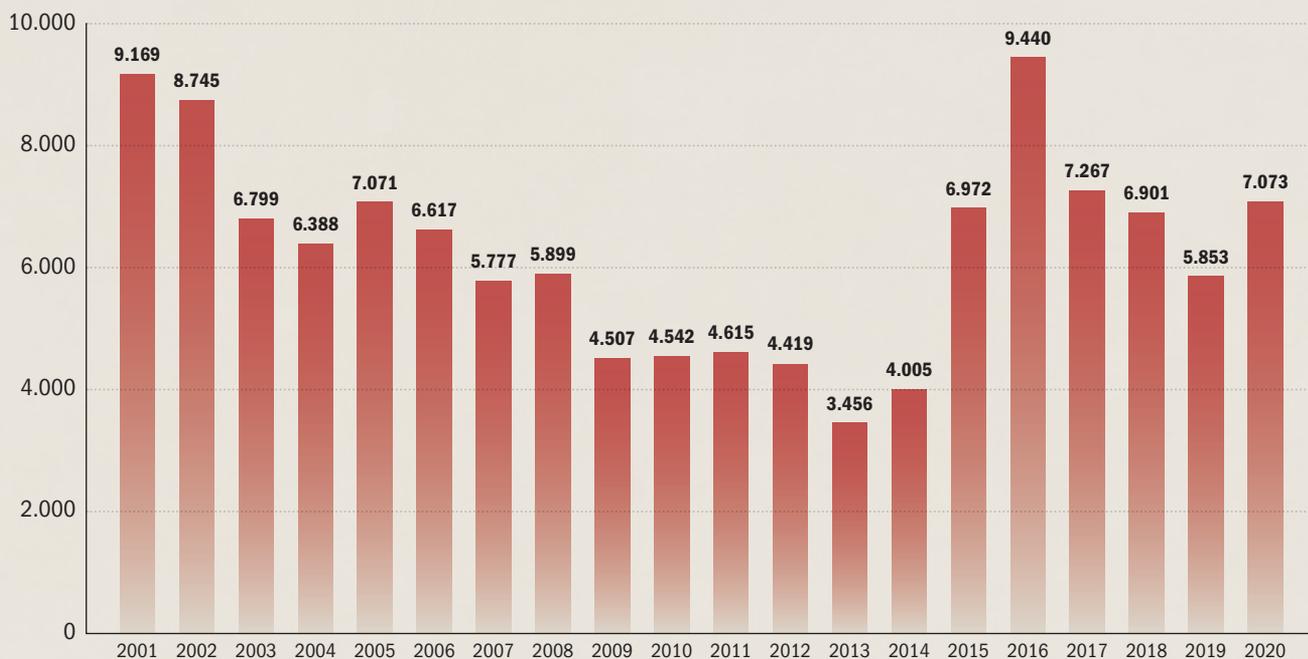
les activités de déminage dans le pays. En 2018, le Zimbabwe a lancé sa stratégie nationale des mesures anti-mines de 2018 à 2025.

Le Zimbabwe possède cinq missions de déminage : l'unité nationale de dégagement des mines de l'Armée nationale du Zimbabwe, HALO Trust, Mines Advisory Group, Norwegian People's Aid (NPA) et l'APOPO (développement d'un produit de détection anti-mines terrestres) belge.

Sten-Trygve Brand, conseiller pour les mesures anti-mines et le désarmement au NPA, déclare que les travaux de déminage de son organisation ont directement aidé plus de 70.000 Zimbabwéens.

« Nous faisons partie des efforts humanitaires de déminage au Zimbabwe depuis 2012... et nous sommes en ce moment actifs avec cinq équipes de déminage et une équipe MDD [détection des mines par les chiens] »,

Nombre total de victimes des mines et des restes explosifs : 2001 à 2020 Source : Landmine Monitor 2021



Talakufa Muzikiti a perdu sa jambe gauche après avoir marché sur une mine terrestre au Zimbabwe. CYRIL ZENDA

« Le dégagement et la libération de la terre le long de la frontière ont permis aux communautés et aux autorités de s'engager dans des activités telles que le contrôle des frontières, l'agriculture, l'accès à l'eau propre, l'accès aux écoles plus près des villages, le pâturage du bétail, ainsi que l'interaction transfrontalière sans menace d'accident qui pourrait conduire à la mort ou la perte d'un membre », déclare le NPA.

Le dégagement des mines terrestres par HALO se concentre dans le Nord-Est du pays, où le groupe travaille depuis 2013 et a détruit plus de 100.000 mines terrestres.

L'organisation déclare : « Ce qui est stupéfiant, c'est que cela représente près de quatre mines terrestres par personne dans cette région du pays. Seulement l'an dernier, l'équipe de HALO au Zimbabwe a dégagé près de 10 % de toutes les mines terrestres détruites dans le monde. »

déclare M. Brand dans un e-mail.

Le NPA a travaillé dans trois champs de mines, d'un total de 16,7 km carrés, sur la frontière orientale avec le Mozambique, c'est-à-dire de Leacon Hill à Sheba Forest, Burma Valley, et de Rusitu à Muzite. Parmi ces trois, le champ de mines de Burma Valley a été dégagé et transféré en 2015, protégeant ainsi 253 foyers. À la fin 2020, le NPA avait détruit 26.982 mines antipersonnel et il lui restait une zone contaminée estimée à 7,2 km carrés, qu'il a l'intention de finir de dégager en 2024.

La faune sauvage menacée est aussi tuée

En plus des morts et des blessures des humains, les mines antipersonnel ont tué plus de 120.000 têtes de bétail. Elles ont aussi tué d'innombrables animaux sauvages, notamment des éléphants, des rhinocéros, des lions et des girafes. Certains champs de mines s'étendent au parc national Gonarezhou, qui fait partie du parc transfrontalier du Grand Limpopo situé dans trois pays. Ce dernier inclut des régions du Mozambique, d'Afrique du Sud et du Zimbabwe, et permet à la faune sauvage de se déplacer en liberté.

Luciã Zuka a perdu sa jambe droite à cause d'une mine terrestre en 1998 lorsqu'elle cherchait du bois de chauffage. CYRIL ZENDA



L'APOPO a commencé ses travaux de déminage en décembre 2020 le long du champ de mines du Cordon Sanitaire qui affecte le corridor de faune sauvage Sengwe dans la région Sud-Est du pays. Il a l'intention de chercher et détruire environ 15.300 mines terrestres et de dégager 7,23 km carrés.

L'organisation déclare : « APOPO pense qu'il devrait pouvoir achever son travail en 2025 ou avant, en fonction du soutien des donateurs. »

« En dégagant les mines terrestres, APOPO peut offrir une fondation solide pour que les communautés rebâtissent leur vie et pour que l'agriculture et l'écotourisme reviennent et prospèrent, en apportant de nombreux bénéfices à tout le pays. »

Les contraintes financières retardent le déminage

L'Armée nationale du Zimbabwe a refusé de fournir des commentaires. Mais il est bien connu que les contraintes financières ont entravé les efforts de déminage. Selon le plan de travail révisé des mesures anti-mines de ZIMAC pour 2020 à 2025 soumis à la Revue des mesures anti-mines, 65,6 millions de dollars sont requis par le programme des mesures anti-mines pour satisfaire à la date limite prolongée à 2025.

ZIMAC a informé la Revue des mesures anti-mines que le ralentissement économique de 2018 limiterait probablement la possibilité pour le gouvernement d'accroître tout financement des mesures anti-mines, bien qu'il anticipe que les niveaux annuels de financement de 500.000 dollars soient maintenus.

Dans le passé, les défis financiers auxquels l'armée zimbabwéenne fait face ont été confirmés par la ministre de la Défense Oppah Muchinguri-Kashiri, laquelle a déclaré que l'armée n'avait même pas les fonds nécessaires pour couvrir ses opérations de base.

Les villageois sont reconnaissants et pleins d'espoir

« Nous sommes heureux pour le processus de déminage qui a lieu, mais le gouvernement devrait trouver un moyen de nous indemniser », déclare M. Mudzikiti dans une interview. Ses sentiments sont partagés par d'autres victimes et par les membres des familles des tués.

Lisimati Makoti, qui est chef Sengwe dans la région de Chikombedzi, a loué l'exercice de déminage des mines terrestres et déclaré que c'est une initiative noble parce que son peuple avait continué à souffrir longtemps après la fin de la guerre.

« Nous sommes reconnaissants de cet exercice de déminage, dit-il. Il était attendu depuis longtemps parce que mon peuple était sujet au risque de perdre la vie à cause des mines terrestres. ... Beaucoup ont aussi perdu leur bétail à cause des mines terrestres. ». □



AU SUJET DE L'AUTEUR

Cyril Zenda est un journaliste basé à Harare (Zimbabwe). Ses écrits ont été publiés dans Fair Planet, TRT World Magazine, The New Internationalist, Toward Freedom et SciDev.Net.



COMMENT CAPTURER UN ÉTAT

LES TACTIQUES HYBRIDES DE LA RUSSIE POUR EXERCER UN CONTRÔLE EN RÉPUBLIQUE CENTRAFRICAINE OFFRENT UN AVERTISSEMENT POUR LE CONTINENT

PERSONNEL D'ADF

De petits nuages de poussière rouge s'élèvent du camion des mercenaires russes qui se dirigent vers le centre de Bambari, en promettant de nourrir les affamés.

Dans la chaleur accablante, des douzaines sont alignés sur un chemin de terre dans la quatrième ville de la République centrafricaine (RCA).

Au lieu de nourriture, ils reçoivent des pancartes fabriquées à la main et sont ordonnés à la pointe du fusil de manifester contre la MINUSCA, la mission de maintien de la paix des Nations unies en RCA, en demandant que l'ONU parte de la ville qu'elle avait libérée des mains des rebelles à la fin 2020.

Cela n'avait pas de sens pour Philip Obaji Jr., journaliste nigérian qui avait fait de longs reportages sur le groupe Wagner, société militaire privée (SMP) russe, à mesure qu'elle développait ses activités en Afrique.

« De multiples sources en RCA m'ont dit que les manifestations anti-ONU dans la ville de Bambari étaient une opération sous fausse bannière, mise en scène par les mercenaires de Wagner, a dit M. Obaji à ADF. Avant qu'un grand nombre de membres de Wagner ne partent

pour l'Ukraine, j'ai fait un reportage traitant des nouveaux impôts sur les produits agricoles qu'ils avaient décrétés et empochés. »

Il a aussi reçu des rapports selon lesquels les mercenaires russes avaient massacré des civils dans les villages de Mouka, Yangoudroudja, Aïgbado et Yanga.

Les accusations d'atrocités suivent le groupe Wagner à la trace.

En RCA, les mercenaires ne sont qu'une composante de l'approche hybride de la Russie, qui combine depuis plus de quatre ans la puissance dure et la puissance souple.

Mattia Caniglia, associé au Conseil européen des relations internationales, a déclaré à ADF : « La RCA est actuellement dans une situation de capture d'état. Le niveau de pénétration que nous constatons est énorme. »

« Pour le moment, vous avez une situation qui est parfaite pour ce que fait la Russie. »

UN PAYS PRÊT À ÊTRE EXPLOITÉ

Les opérateurs russes sont en RCA depuis 2017 ; ils sont venus après avoir traversé la frontière poreuse du Nord-Est avec le Soudan. Ils se sont enracinés en tirant profit



Un instructeur militaire russe travaille avec un membre des Forces armées de Centrafrique.

COMMUNAUTÉ DES OFFICIERS POUR LA SÉCURITÉ INTERNATIONALE

À DROITE : Un instructeur militaire russe parle à une unité des Forces armées de Centrafrique.

COMMUNAUTÉ DES OFFICIERS POUR LA SÉCURITÉ INTERNATIONALE

de l'instabilité générale, des sentiments anti-français, et de Faustin-Archange Touadéra, le président qui était sur le point d'être renversé par les rebelles.

Pendant plus de quatre ans, la Russie a gagné un accès sans précédent aux leviers du pouvoir gouvernemental et l'ont utilisé pour diffuser leur propagande, en laissant de nombreux habitants incertains quant à ceux en qui on pouvait faire confiance dans le pays.

M. Caniglia décrit l'approche de la Russie en Afrique comme étant opportuniste et stratégique, en mettant l'accent sur l'importance de distinguer entre ses deux piliers : les activités officielles et non officielles.

« Pour le non-officiel, nous avons beaucoup de choses asymétriques, hybrides, dit-il. Pour l'officiel, nous les avons aussi, mais il s'agit surtout d'accords bilatéraux, de formation militaire, de contrats d'armement et plus encore. »

L'approche de la Russie est très nettement visible en RCA.

En 2018, le président Touadéra a installé Valery Zakharov, ex-agent russe des renseignements lié au Kremlin, comme conseiller pour la sécurité nationale.

L'Union européenne (UE) a appelé M. Zakharov « un personnage clé dans... la structure de commandement du groupe Wagner », qui maintient « des liens étroits avec les autorités russes. »

Le pouvoir que Wagner a acquis en RCA pourrait même avoir dépassé ses attentes.

« C'est quelque chose qui est plutôt sans précédent, déclare M. Caniglia. Mais encore une fois, toutes les conditions étaient présentes en RCA. Ils ont acquis une influence qu'ils ne sont pas autorisés à avoir dans tout autre lieu. »

Alexander Ivanov, autre allié du président, a aussi des liens étroits avec Wagner, selon des rapports.

En tant que représentant officiel des formateurs militaires russes en RCA, M. Ivanov dirige un groupe indépendant de « défense de la paix » appelé Communauté des officiers

pour la sécurité internationale (COSI).

Le ministère de la Défense russe admet qu'il a utilisé M. Ivanov pour recruter tous les formateurs déployés pour entraîner les Forces armées de Centrafrique (FACA), selon la déclaration de la Russie devant un panel d'experts de l'ONU.

L'emploi d'agents commerciaux privés tels que Wagner et COSI fournit à la Russie la couverture nécessaire. Sa capacité de nier une participation officielle est une pièce cruciale du puzzle délibérément opaque que constitue l'approche hybride de la Russie en RCA.

Kevin Limonier, maître de conférences en géopolitique et spécialiste du cyberspace russophone, a déclaré au magazine *The Africa Report* : « Leur motivation est principalement financière. Ils considèrent que l'Afrique est un lieu pour gagner de l'argent et explorer de nouveaux horizons. »

Le modèle hybride de la Russie lui permet d'exercer de l'influence avec un faible investissement en argent et main d'œuvre.

« L'État russe n'a pas nécessairement les moyens de réaliser ses ambitions politiques en Afrique, déclare le professeur Limonier. C'est pourquoi il s'appuie sur ces réseaux qui utilisent des méthodes non conventionnelles et nie leur participation en cas de problème. »

Avec le groupe Wagner, les problèmes surviennent toujours.

LE POUVOIR DUR : FORMATEURS ET MERCENAIRES

Avec des effectifs estimés entre 2.200 et 3.000, Wagner est la plus connue de plusieurs SMP russes actives comme formateurs et fournisseurs de sécurité.

Chaque fois que le président Touadéra ou d'autres officiels de haut rang sortent en public, des gardes lourdement armés en tenue de treillis ne sont pas loin. Ils se déplacent dans des véhicules russes blindés et ils coordonnent occasionnellement avec des hélicoptères et des drones russes.

Le Bureau de l'ONU pour la coordination des affaires humanitaires estime que 3,1 millions de personnes, soit plus de 60 % de la population de la RCA, nécessitent un secours urgent. Le nombre de déplacés internes a augmenté à un chiffre record de 722.000, et 733.000 personnes de plus se sont réfugiées dans d'autres pays.

Un transport de troupes blindé russe est livré aux Forces armées de Centrafrique à Bangui le 15 octobre 2020.

AFP/GÉTTY IMAGES





Alexander Ivanov s'exprime lors de la projection à Bangui du film de propagande « Touriste » du groupe Wagner, qui a été filmé en République centrafricaine.

COMMUNAUTÉ DES OFFICIERS POUR LA SÉCURITÉ INTERNATIONALE

À DROITE : M. Ivanov parle à un groupe de journalistes locaux.

COMMUNAUTÉ DES OFFICIERS POUR LA SÉCURITÉ INTERNATIONALE



Ce qui avait commencé comme une mission de formation en 2018 s'est finalement transformé en opérations anti-insurrectionnelles avec des mercenaires russes sur le terrain, qui dirigent dans certains cas les unités FACA.

Les rapports de massacres perpétrés par les mercenaires russes et les troupes FACA qui suivent leurs ordres ont déstabilisé l'armée.

En juin 2020, un panel d'experts de l'ONU a déclaré qu'il avait « reçu de nombreux rapports sur les formateurs russes qui tuaient sans discrimination les civils non armés », utilisaient une force excessive et pillaient en RCA, particulièrement dans les régions minières.

Le panel a aussi déclaré que des mercenaires libyens et syriens étaient engagés dans les combats aux côtés des formateurs russes.

En mars 2021, le Haut-Commissariat des Nations unies aux droits de l'homme a reçu des rapports concernant des exécutions en masse, des tortures, des détentions arbitraires, des relocalisations forcées des civils et des attaques contre le personnel humanitaire attribuées aux SMP travaillant avec FACA, y compris le groupe Wagner.

LE POUVOIR SOUPLE : GUERRE DE L'INFORMATION

La Russie a employé plusieurs procédés du pouvoir souple pour promouvoir son agenda en RCA.

Par l'intermédiaire des mercenaires, des sociétés fantômes et autres agents, la Russie a financé des médias locaux, parrainé des acteurs influents « anti-impérialistes », produit de la propagande multimédia et conduit des campagnes de désinformation et mésinformation.

Il est signalé que les membres du groupe Wagner et leurs associés ont construit des terrains de jeu et des statues en leur propre

honneur. Ils ont créé au moins deux films de propagande du groupe Wagner en RCA pour idéaliser leurs actes. Ils ont organisé des tournois de foot et des concours de beauté.

L'oligarque Evgueni Prigojine, lié au Kremlin et accusé par l'UE de financer le groupe Wagner, a subventionné la création de la station de radio Lengo Songo (qui signifie « Développer la solidarité » en sango) avec 10.000 dollars, selon la BBC. La station a une position fortement pro-russe et blâme l'ONU et la France pour la crise de la RCA.

Les mercenaires russes sont accompagnés d'un éventail de services médiatiques.

« Ils ne coûtent pas grand-chose et sont fournis dans le cadre d'un ensemble de services de soutien au régime, y compris des technologies politiques », déclare au sujet de Wagner Mark Galeotti, expert en affaires de sécurité russes, au journal indépendant The Moscow Times.

Le financement russe et les campagnes de manipulation des médias ont aidé M. Touadéra à être réélu en 2020 avec une marge confortable.

On signale que M. Zakharov a supervisé la nomination des alliés de M. Touadéra aux postes clés pendant les élections, y compris le décompte des votes.

La RCA est l'un des huit pays africains où Facebook, le géant des réseaux sociaux, a suspendu des centaines de comptes frauduleux et démantelé ce qui était selon lui des campagnes russes d'interférence dans les élections. En RCA, des trolls russes ont diffamé les pays africains voisins et les partenaires étrangers tout en présentant la Russie comme un libérateur.

Il s'ensuit des manifestations de rue coordonnées ciblant la France, la MINUSCA et la Communauté économique des États de l'Afrique centrale.

En août 2021, la MINUSCA a aussi été ciblée par de fausses rumeurs selon lesquelles elle fournissait des mines terrestres aux rebelles, alors même qu'elle déployait son personnel pour éliminer ces engins.

« La MINUSCA n'a jamais utilisé de mines » a déclaré à la BBC le major Ibrahim Atikou Amadou, porte-parole des forces de l'ONU, en notant que les opérations de déminage avaient atteint une impasse à cause des allégations.

LE POUVOIR DIPLOMATIQUE

La Russie, utilisant sa position au Conseil de sécurité de l'ONU, a pris pied pour la première fois en RCA lorsque l'ONU a levé un embargo sur les armes, ce qui a permis à la Russie de vendre des armes dans le pays.

Des efforts russes plus récents, notamment le blocage des nominations aux panels d'experts de l'ONU et la subversion conséquente du processus de sanctions internationales, ont enrayé les investigations dans les activités de la Russie et ses SMP.

Richard Gowan, directeur de l'International Crisis Group aux Nations unies, a déclaré au magazine *Foreign Policy* : « Il semble que Moscou souhaite paralyser les sanctions et les panels d'experts pour détourner l'attention de ce que fait Wagner en Afrique. Dans certains cas, c'est tout simplement une façon de dissimuler des actes répréhensibles. »

LE PRIX PAYÉ PAR LA RCA

L'obtention de concessions lucratives de mines d'or, de diamant et d'uranium est une grande priorité pour les opérateurs russes en RCA. Sans compte-rendu du gouvernement concernant les paiements accordés aux formateurs ou aux SMP russes, les experts pensent que les concessions minières sont accordées en échange du service des mercenaires.

Les activités d'extraction de la grande richesse minérale de la RCA sont prises en charge par les sociétés fantômes russes telles que Lobaye Invest, qui est liée directement à M. Prigojine et a été créée en octobre 2017, avec une SMP filiale appelée Sewa Security Services.

Léopold Mbolli Fatran, ministre des Mines de Centrafrique, a accordé à Lobaye des permis d'exploration minière dans deux régions en juin et juillet 2018. Il a fini par octroyer des permis dans six régions : Alindao, Birao, Bria, N'Délé, Pama et Yawa.



M. Obaji et d'autres journalistes ont lié les massacres perpétrés par les mercenaires aux nombreux sites miniers, alors que les Russes essaient de sécuriser leurs concessions.

Là où les Russes étaient jadis célébrés, ils découvrent maintenant que les villageois ont peur de leur arrivée.

« Il y a environ deux ou trois ans, les gens étaient relativement heureux que les Russes soient là, déclare M. Caniglia. Mais maintenant ils savent ce qui se passe. »

Le Bureau de l'ONU pour la coordination des affaires humanitaires estime que 3,1 millions de personnes, soit plus de 60 % de la population de la RCA, nécessitent un secours urgent. Le nombre de déplacés internes a augmenté à un chiffre record de 722.000, et 733.000 personnes de plus se sont réfugiées dans d'autres pays.

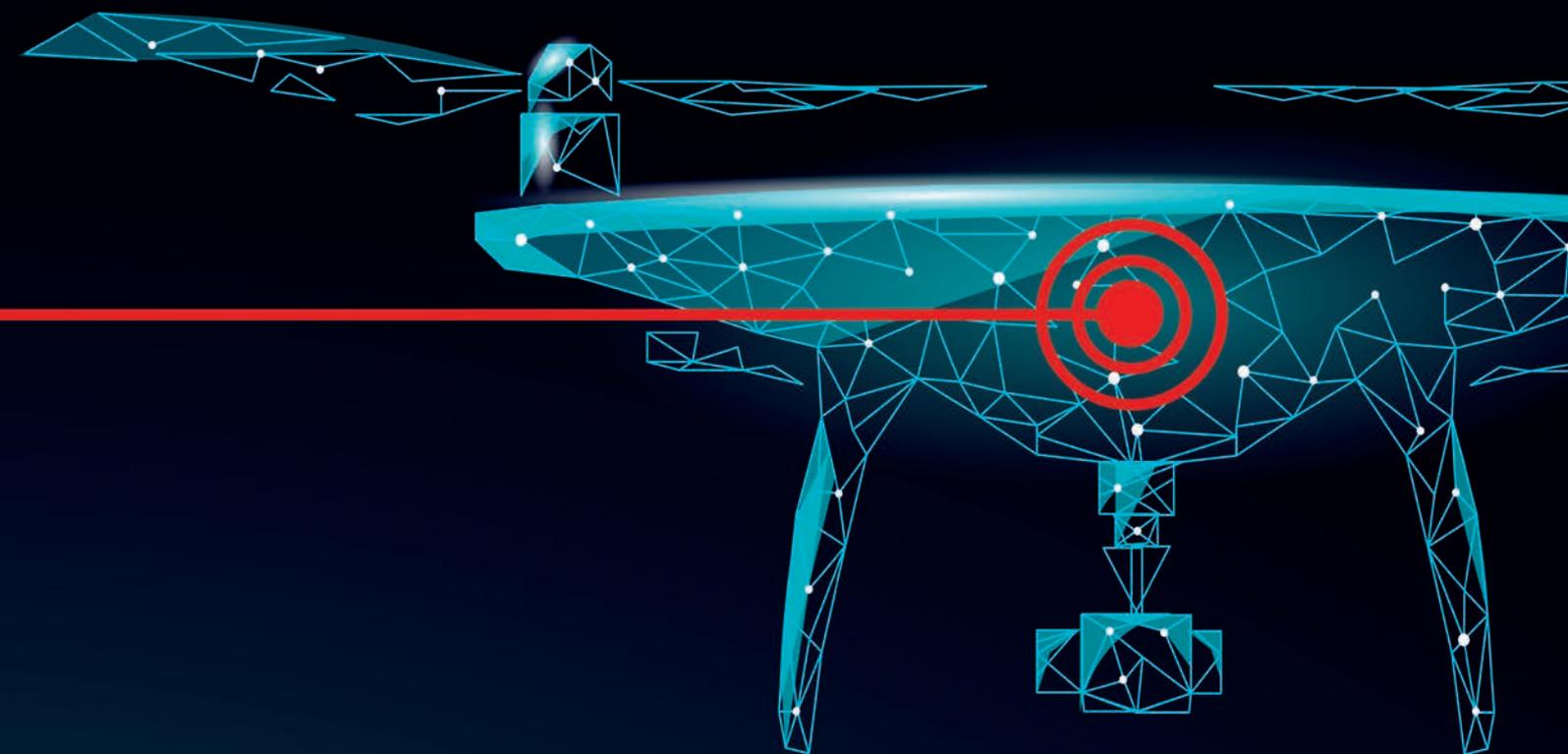
De tels résultats après plus de quatre ans d'engagement russe en RCA pourraient servir d'avertissement aux autres pays africains envisageant des mercenaires, déclare M. Caniglia.

« Mais ce n'est pas ce qui se produit. » Certains pays de la région du Sahel signalent qu'ils sont ouverts à l'idée d'accueillir les forces russes, malgré les antécédents clairs de ces dernières pour provoquer l'instabilité. Les observateurs sont surpris que ces pays ne tirent pas les leçons de la RCA sur les dangers d'un partenariat avec Wagner et la Russie.

« Ce qui se passe en RCA est très mauvais, non seulement en ce qui concerne le niveau d'influence que les acteurs russes non étatiques détiennent sur le gouvernement de la RCA, mais aussi en termes des abus des droits humains et de la déstabilisation croissante de la situation sécuritaire. Mais le message n'est pas transmis. Il reste tout simplement ignoré », déclare M. Caniglia. □

Il est estimé que Faustin-Archange Touadéra, président de la République centrafricaine, a demandé pour la première fois au président russe Vladimir Poutine une assistance militaire lors de la Conférence au sommet Russie-Afrique de 2019 à Sochi.

AFP/GETTY IMAGES



LES DRONES PEUVENT ÊTRE DES ARMES MORTELLLES POUR LES EXTRÉMISTES

Les terroristes emploient des drones pour identifier les cibles et conduire la surveillance en Afrique. La prochaine étape consistera à les militariser.

La technologie des drones, peu chère et largement disponible, pourrait potentiellement révolutionner la livraison des médicaments, le traitement des récoltes et la surveillance en Afrique. Mais là où les innovateurs voient des opportunités d'améliorer la vie des gens, les groupes extrémistes voient la possibilité de la détruire.

Au Moyen-Orient, les groupes terroristes ont commencé à militariser les drones standards pour attaquer les cibles civiles et militaires. Aujourd'hui, avertissent les experts, cette tactique meurtrière pourrait venir en Afrique.

Aaditya Devarakonda, PDG de DEDRONE, a déclaré au magazine Forbes à propos des drones : « Pour 2.000 dollars, vous pouvez franchir toutes les barrières du monde. C'est la menace la plus asymétrique qui existe ». DEDRONE sécurise l'espace aérien pour protéger les organisations contre les drones malveillants.

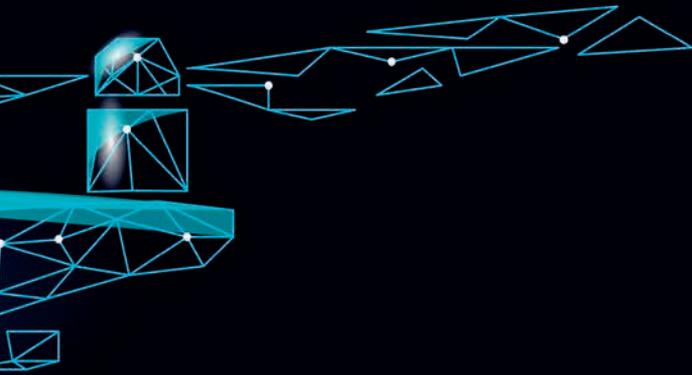
Les drones télécommandés, appelés aussi systèmes aériens sans humain à bord, remontent au milieu des années trente. Aujourd'hui, les drones sont de toute taille, depuis les petits jouets de 30 dollars contrôlés par radio jusqu'aux aéronefs de la taille d'un avion. Entre les deux extrêmes, on constate un éventail stupéfiant d'appareils capables de transmettre les vidéos, de surveiller les mouvements des troupes et de transporter les cargaisons.

La sophistication des drones commerciaux « d'amateur » est étonnante. Un simple drone qui coûte moins de 1.000 dollars possède quatre moteurs rechargeables d'une autonomie de vol de 30 minutes, une caméra à trois degrés de liberté produisant des vidéos à haute résolution, un capteur capable de filmer des vidéos de nuit et une portée de transmission vidéo de plus de 11 km.

La plupart des drones peu coûteux ne peuvent pas transporter une charge de plus de 2 kg, mais de nombreuses sociétés ont développé des drones capables de transporter jusqu'à 200 kg. Le prix courant de ces drones est d'environ 250.000 dollars. Ceci démontre la progression du développement des drones au 21^{ème} siècle : il y a vingt ans, un drone ayant cette capacité et ce prix aurait été inconcevable.

Le rédacteur scientifique Kashyap Vyas déclare qu'une « énorme explosion » dans le développement des drones s'est produite au cours des dix dernières années.

M. Vyas a écrit pour le site web Interesting Engineering : « Il est anticipé que les drones vont devenir plus petits et plus légers, avec une autonomie de batterie et un temps de vol beaucoup plus



longs. Dans le marché civil, les développements visant à améliorer le temps de vol leur permettent d'être employés comme plateformes de livraison, dans les services d'urgence et pour la collecte des données dans un certain nombre de zones trop dangereuses pour les êtres humains, par exemple dans les centrales électriques ou les incendies. »

Certains décrivent aujourd'hui la technologie des drones comme une boîte de Pandore moderne : ce qui avait commencé comme outil pour la photographie aérienne et autre s'est développé et a évolué de différentes façons, positives et terribles.

LES DRONES EN AFRIQUE

Jusqu'à présent, il n'existe pas de rapport de drones militarisés employés par les groupes terroristes en Afrique, mais les experts avertissent que cela pourrait changer rapidement.

Murtala Abdullahi, journaliste nigérian qui traite des questions de sécurité pour le site HumAngle, déclare que l'accès aux drones est étroitement réglementé au Nigeria, et donc les groupes extrémistes ont recours à la capture des drones du gouvernement. Pour le moment, ils ont été surtout utilisés pour des efforts de surveillance et de propagande, mais il dit que les groupes ont l'intention d'accroître leur emploi et veulent apprendre auprès des groupes extrémistes du Moyen-Orient.

M. Abdullahi a déclaré lors d'un webinaire du Centre africain pour les études stratégiques (ACSS) : « Ce n'est pas aussi sophistiqué qu'au Moyen Orient, où les drones ont été équipés d'explosifs pour cibler les troupes, mais cela ne veut pas dire que nous ne verrons pas cela à l'avenir. La technologie de l'information a permis à ces groupes d'obtenir des connaissances auprès d'autres régions ; cela veut dire que la possibilité qu'ils amélioreront ce qu'ils ont déjà en apprenant auprès des autres constitue un risque énorme. »

Au Mozambique, les extrémistes de la province du Cabo Delgado utilisent des drones à des fins de surveillance. Amade Miquidade, ministre mozambicain de l'Intérieur à l'époque, a signalé en 2020 que les extrémistes avaient déployé des drones dans une région où une force de stabilisation de la Communauté de développement d'Afrique australe avait été autorisée à entrer.

Pendant les attaques extrémistes de la fin mars et du début avril 2021 qui ont ciblé la municipalité stratégiquement importante de Palma, entre autres, M. Miquidade a déclaré que les militants employaient des drones pour améliorer la précision des attaques.

« Si nous examinons la facilité avec laquelle [les insurgés] obtiennent des armes et organisent des attaques contre les forces armées, je



Des policiers somaliens et un soldat ougandais observent un drone lors d'une session de formation.

REUTERS



REUTERS

UN HISTORIQUE DES DRONES **MILITARISÉS**

L'utilisation par les terroristes des drones comme armes remonte à près de dix ans. Voici quelques attaques connues employant des drones :

- Al-Qaïda a utilisé de multiples drones en 2013 au Pakistan lors d'une attaque qui a échoué.
- L'État islamique a utilisé de petits drones dans des attaques en Irak et en Syrie en 2014.
- L'État islamique a utilisé des drones pour bombarder les soldats irakiens avec des explosifs légers pendant la bataille de Mossoul en 2016 et 2017.
- Un essaim de drones armés de bombes a attaqué les bases russes de l'Ouest de la Syrie en janvier 2018. Dix drones transportant des explosifs ont attaqué une base aérienne russe alors que trois autres ont ciblé une installation navale russe.
- Des drones armés ont attaqué deux stations de pompage de pétrole en Arabie saoudite en mai 2019. Les officiels ont accusé les rebelles houthis du Yémen d'avoir commis l'attaque. Quelques mois après, les forces houthistes ont lancé des attaques par drone contre trois bases aériennes saoudiennes. Les sources houthistes déclarent que les drones ont atteint leurs cibles mais les officiels saoudiens disent que les drones ont été interceptés et abattus.
- Des drones houthis ont attaqué deux installations de pétrole majeures en Arabie saoudite en septembre 2019, en provoquant des incendies.
- Le 14 septembre 2019, les Houthis ont lancé des attaques par drone contre deux installations de pétrole majeures gérées par Saudi Aramco et ont provoqué un incendie.
- Des terroristes basés au Pakistan ont utilisé deux drones armés pour attaquer une base aérienne indienne en juin 2021.



ne sous-estimerai jamais la possibilité qu'ils commencent à employer des capacités technologiques plus avancées, qui incluent les drones », a déclaré Jasmine Opperman, consultante sud-africaine en sécurité, dans un article d'ACSS. Mme Opperman ajoute : « Si vous pouvez amener des centaines de téléphones cellulaires en contrebande illégale, qu'est-ce qui les empêche d'amener des drones ? »

Les experts avertissent aussi que les drones pourraient remplacer les kamikazes.

Le major Thomas Pledger, officier d'infanterie dans la Garde nationale de l'Armée de terre des États-Unis, écrit : « Les groupes terroristes néces-

Le colonel David Peddle (à la retraite), ancien membre de la Force nationale de défense d'Afrique du Sud, a confirmé que les acteurs non étatiques armés ont employé des drones à des fins de surveillance et pense que « tôt ou tard » on verra le déploiement des essaims ou des faisceaux de drones offensifs en Afrique, étant donné leur accessibilité et leur coût relativement économique.

D'autres experts en conviennent, en déclarant que la technologie et l'industrie manufacturière modernes ont rendu les drones de plus en plus accessibles aux terroristes. Dans son livre « Life 3.0 », le physicien Max Tegmark écrit : « il est probable que le coût des petits drones assassins



Un technicien inspecte un drone de surveillance exploité par les Nations unies en République démocratique du Congo. REUTERS

sitent des personnes pour exécuter leurs attaques. De nombreux groupes conduisent en général des attaques en anticipant que leurs membres se sacrifieront pendant l'attaque, en étant capturés ou tués. Toutefois, l'emploi des drones peut permettre à une personne ou un petit groupe de conduire plusieurs attaques sans sacrifice personnel. »

Une préoccupation majeure, déclarent les experts des drones, est le fait que les développements dans la technologie des drones coïncident avec les avancées en intelligence artificielle (IA). L'emploi de l'IA pourrait conduire à des drones qui n'ont pas besoin d'opérateur. Les experts envisagent que les extrémistes utiliseront des « essaims » de petits drones peu coûteux avec IA dans des attaques ciblées.

propulsés par l'IA dépassera à peine celui des smartphones. »

En outre, les drones réduiront au minimum les investissements en ressources humaines requis pour les attaques terroristes. Les chercheurs notent que la plus grande autonomie permettra à une seule personne d'infliger davantage de dommages. L'IA pourrait rendre le terrorisme plus économique et réduire le coût humain requis pour conduire les attaques, ce qui créera une nouvelle génération de « loups solitaires » terroristes.

La technologie nécessaire pour attaquer les personnes (logiciel de reconnaissance faciale, drones et « machine to machine ») existe déjà. Le Dr Tegmark a imaginé des drones assassins économiques avec IA, dignes d'un film de James Bond :

« Il leur suffit simplement de charger la photo et l'adresse de leur cible dans le drone assassin ; il peut ensuite s'envoler vers la destination, identifier et éliminer la personne, et s'autodétruire pour assurer que personne ne sache qui est responsable. »

Le chercheur Jacob Ware, écrivant pour le site web de sécurité War on the Rocks, déclare que la combinaison d'une simple IA et des drones fait peser une véritable menace sur le monde.

« Les groupes terroristes emploient de plus en plus dans les attaques les technologies du 21^{ème} siècle, notamment les drones et l'intelligence artificielle de base, selon lui. Alors que sa militarisation continue, l'IA pourrait devenir une menace

infectieuses sont très répandues et les craintes sont bien connues. »

Le major Pledger prédit que les drones, à cause de leur « coût relativement faible » et de la distance « importante » à laquelle ils peuvent être déployés, seront utilisés comme « principale tactique dans les attaques terroristes futures ».

« L'infrastructure critique est aussi vulnérable et le renforcement de milliers d'emplacements contre une attaque serait dans le meilleur des cas une limitation financière. Les cibles d'infrastructure probables comprennent les installations de stockage de carburant ou d'eau, les gazoducs, les centrales de distribution électriques et les lieux



Un technicien lance un drone au Rwanda dans le cadre d'un programme qui les emploie pour livrer les fournitures médicales dans les zones rurales. AFP/GETTY IMAGES

formidable en permettant à des adversaires, y compris des acteurs non étatiques, d'automatiser les massacres à une échelle massive. La combinaison de l'expertise des drones et de l'IA plus sophistiquée pourrait permettre aux groupes terroristes d'acquiescer ou de développer des armes autonomes létales, ou "robots assassins", qui accroîtraient dramatiquement la capacité de créer des incidents de destruction massive dans les villes de l'Occident. »

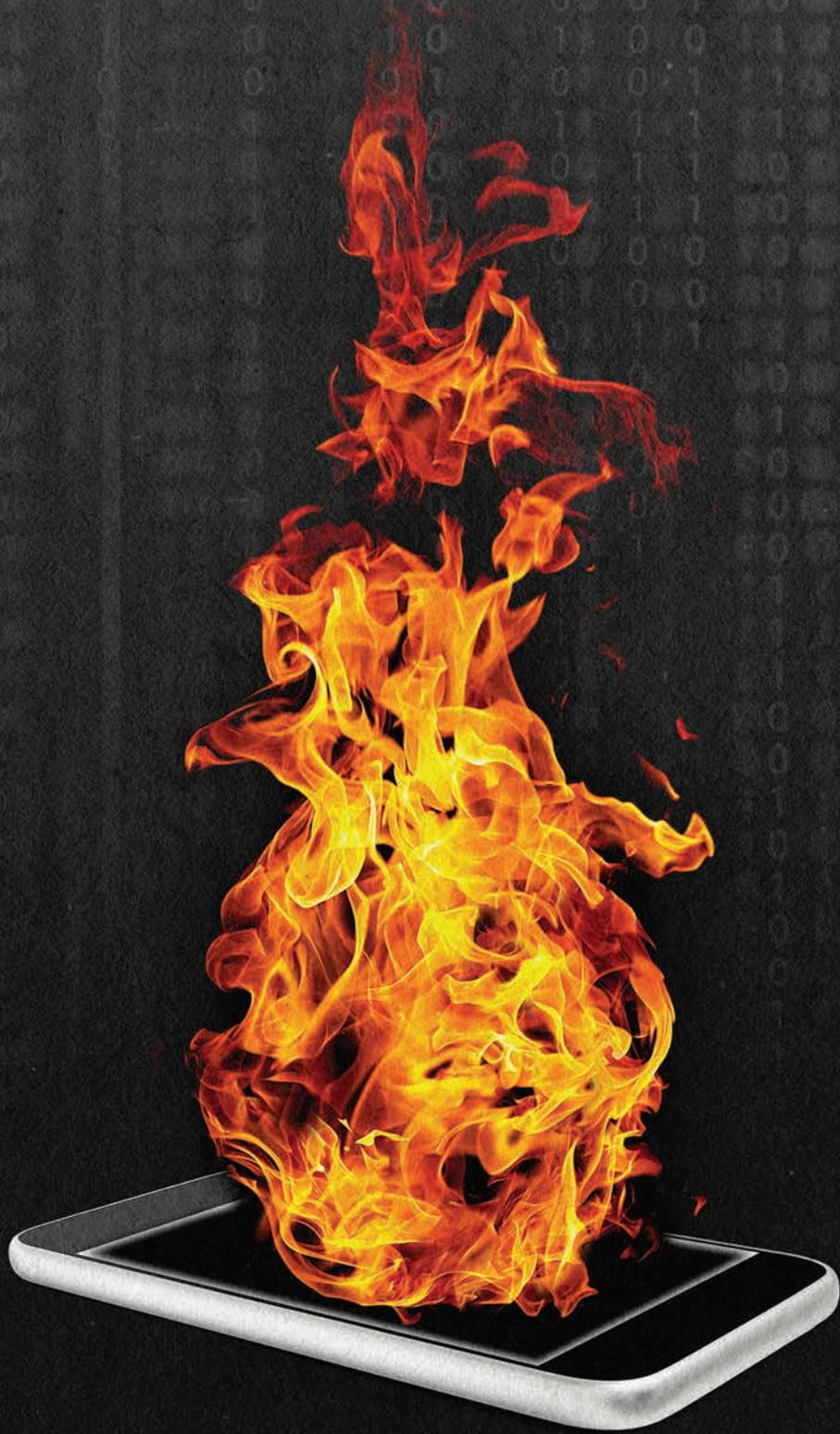
Dans son étude, le major Pledger note que les drones offrent un nouvel éventail de tactiques et de cibles terroristes.

« Une application particulièrement effrayante des drones est la diffusion des agents chimiques et biologiques, tout spécialement les maladies infectieuses, écrit-il. Les conversations sur les maladies

d'approvisionnement alimentaire. Beaucoup d'entre elles ont peu de personnel, ou n'en ont pas du tout. »

Karen Allen, experte de la sécurité pour l'Institut pour les études de sécurité d'Afrique du Sud, déclare que les drones représentent « une nouvelle itération de la technologie du numérique et l'Afrique en fera partie ».

« Bien que la technologie des drones soit largement employée à des fins positives, la possibilité que des personnes construisent des drones avec des smartphones et un logiciel open source s'accroîtra et les résultats pourraient être déstabilisateurs. En bref, il est probable que les drones fassent partie intégrante des guerres africaines du futur. » □



L'AFRIQUE AFFRONTE DES ENNEMIS À HAUTE TECHNOLOGIE

*Les extrémistes
militarisent
la technologie,
les réseaux sociaux et
même les jeux vidéo
dans leurs attaques*

PERSONNEL D'ADF

Plus de trente sites web au Mozambique, y compris celui du ministère de la Défense, ont été mis hors service le 21 février 2022 après avoir été ciblés par des hackers.

L'image d'un homme portant un foulard et brandissant une mitrailleuse est apparue sur le site avec la phrase « piraté par les hackers du Yémen ». Les cibles comprenaient les portails des agences de gestion des catastrophes nationales, de l'administration routière et des services d'eau, ainsi que le ministère de la Défense et l'Institut national du transport terrestre.

Les officiels ont déclaré qu'aucune information n'avait été perdue, et qu'aucune donnée personnelle n'avait été divulguée, mais ils ont noté que c'était la première attaque cybernétique de cette ampleur contre le pays. Les analystes ont demandé au gouvernement de renforcer la cybersécurité et craignent que les hackers ne soient associés à des terroristes.

Alors que les experts et les chercheurs avertissent que les extrémistes africains utiliseront des technologies facilement disponibles à l'avenir pour faire avancer leurs objectifs, d'autres experts déclarent que cela s'est déjà produit.

Les extrémistes se servent des drones pour la surveillance. Ils se servent des réseaux sociaux à des fins de propagande et pour diffuser en direct les événements. Ils produisent des vidéos à des fins de recrutement et d'instruction. Ils utilisent des outils de communication pour planifier des raids. À l'avenir, déclarent les experts, les drones commerciaux seront militarisés et les imprimantes 3D seront employées pour fabriquer des fusils d'assaut.

Tout commence avec l'outil le plus courant et le plus polyvalent : le téléphone cellulaire. Comme l'a noté l'auteur Audrey Kurth Cronin lors d'une présentation en mai 2021 par le Centre africain pour les études stratégiques (ACSS), « tout le monde possède un ordinateur performant dans sa poche ».

Un smartphone ne semblerait pas être une arme redoutable, ni même une arme particulièrement sophistiquée, mais il combine un ordinateur, une horloge de précision, une caméra, l'accès à l'Internet, le GPS, des applications de transfert d'argent et plus encore. Il élimine aussi la nécessité pour les insurgés de maintenir un équipement de communication radio.



Des hackers chinois ont volé les informations des serveurs de l'Union africaine et transmis les données à Shanghai. REUTERS

Les extrémistes emploient les téléphones mobiles pour toute une gamme d'objectifs, selon les experts. L'un de ceux-ci est l'acceptation des paiements et du transfert d'argent comptant lorsqu'ils extorquent des « paiements de taxe » auprès des citoyens dans les zones reculées qu'ils contrôlent.

Le chercheur Seth Harrison, qui écrit pour le Centre pour les études stratégiques et internationales, indique que les groupes tels que l'État islamique tirent profit de la technologie facilement disponible à des fins de propagande et d'instruction.

La fumée s'élève du centre commercial Westgate de Nairobi (Kenya) en 2013 à la suite d'une attaque terroriste. Les terroristes ont diffusé leur attaque sur Twitter. THE ASSOCIATED PRESS



« Ces opérations exigent une formation ou une planification tactique réduite, concernent des outils de base (par exemple des couteaux ou des voitures) et peuvent être exécutées par n'importe qui, n'importe où. La combinaison des opérations simples et d'une capacité de communication accrue a rendu le terrorisme accessible au plus grand nombre. »

Deux frères ont utilisé la vidéo en ligne « Comment construire une bombe dans la cuisine de ta mère », produite par al-Qaïda, pour fabriquer une bombe qu'ils ont déclenchée lors du marathon de Boston en 2013.

Les experts en technologie avertissent que les extrémistes employant des drones commerciaux aisément disponibles peuvent conduire une surveillance et planifier des attaques. À l'avenir, déclarent-ils, les drones pourraient être utilisés en Afrique pour transporter de petites quantités d'explosifs et effectuer des assassinats.

DÉJÀ EN COURS D'UTILISATION

Il est utile de distinguer deux types de technologie : la technologie ouverte et la technologie fermée. La technologie fermée est mise à la disposition presque exclusive des états. Elle inclut les armes nucléaires, les armements majeurs, les avions de combat à réaction et le radar. La technologie ouverte est à la portée de tous. Elle inclut les systèmes GPS, l'Internet, les smartphones et les puces électroniques. Bien que la technologie fermée tombe occasionnellement entre les mains des extrémistes, c'est en général la technologie ouverte qui provoque les problèmes les plus graves.

Les acteurs non étatiques constituent la principale préoccupation, mais il existe d'autres problèmes. Comme l'a remarqué Nathaniel Allen de l'ACSS dans



Un garde de sécurité en patrouille au centre commercial Westgate de Nairobi (Kenya) près de deux ans après une attaque terroriste.

THE ASSOCIATED PRESS

un rapport de janvier 2021, « les plus grandes craintes concernant l'espionnage cybernétique en Afrique ont été liées à la Chine ».

En 2018, il a été signalé que tout le contenu des serveurs au siège social de l'Union africaine était habituellement retransmis à Shanghai (Chine) lorsque les ingénieurs du réseau ont noté une pointe d'utilisation pendant les heures non ouvrées. Bien que les ingénieurs aient remplacé les serveurs, les hackers chinois ont continué à espionner l'UA en 2020 en détournant les films des caméras de surveillance. Ils ont dissimulé leur piste en retransmettant les informations à la Chine pendant les heures ouvrées normales. Un groupe de hackers chinois appelé Bronze President en est responsable. Selon Reuters, la surveillance concernait « les bureaux de l'UA, les aires de stationnement, les couloirs et les salles de réunion ».

En juin 2020, l'agence éthiopienne de sécurité des

réseaux d'information a arrêté une attaque cybernétique effectuée par le groupe Cyber Horus basé en Égypte. Le Dr Allen a écrit que l'attaque faisait, selon les autorités éthiopiennes, partie d'une tentative visant à exercer « des pressions économiques, psychologiques et politiques sur l'Éthiopie » liée au remplissage du Grand Barrage de la renaissance éthiopienne sur le Nil.

Les autorités éthiopiennes disent qu'elles ont prévenu une attaque plus vaste. Pourtant, le groupe Cyber Horus a réussi à pirater une douzaine de pages web du gouvernement, en affichant des messages menaçant la guerre si l'Éthiopie commençait à remplir le barrage.

UN MANQUE DE TECHNOLOGIE

Anouar Boukhars, professeur de contreterrorisme et de lutte contre l'extrémisme violent à l'ACSS, remarque que les extrémistes africains utilisent la cybertechnologie à des fins de formation, propagande, recrutement, financement et planification. Il déclare que les extrémistes utilisent la technologie de l'information pour contrôler le rythme et le récit de la violence, et que Boko Haram avait commencé à employer le sabotage cybernétique dès 2012.

Le professeur Boukhars déclare que la plupart des attaques cybernétiques des extrémistes en Afrique ne sont pas particulièrement sophistiquées. Bien que l'on puisse supposer que les extrémistes souhaiteraient acquérir des drones de qualité militaire, il dit que la construction, l'opération et la surveillance de tels appareils sont coûteuses. Il est plus probable que les extrémistes utiliseront des drones de qualité commerciale. Même les opérations militaires avancées des gouvernements commencent à utiliser des drones civils.

Le Dr Christopher Anzalone, professeur adjoint de recherche à l'université du Corps des fusiliers marins de Quantico (Virginie), déclare qu'al-Shebab est l'un des groupes extrémistes les plus agressifs dans l'adoption de la technologie à des fins de recrutement. La présentation raffinée de leurs films de propagande ressemble à des « pseudo-documentaires », dit-il.

Il déclare qu'al-Shebab continue aussi à employer des moyens de bas niveau technologique (émissions radio et photographie simple) pour transmettre son message. Mais il note que le groupe a rapidement adopté Twitter et a diffusé en direct sur ce réseau en 2013 son attaque du centre commercial Westgate de Nairobi (Kenya), où 67 personnes ont trouvé la mort avant que quatre tireurs masqués ne soient tués.

LES JEUX VIDÉO

Une étude de l'université de Caroline du Nord à Chapel Hill révèle que les groupes terroristes se procurent des composantes des jeux vidéo populaires, en particulier la série populaire Call of Duty, pour les employer à des fins de recrutement et de pratique. Les jeux vidéo de tir à la première personne sont joués par des millions de personnes, en général de moins de trente ans, dont une

INTERPOL IDENTIFIE LES PRINCIPALES MENACES AFRICAINES

Le Rapport d'évaluation des cyber-menaces africaines 2021 d'Interpol identifie les menaces les plus proéminentes en Afrique, en fonction des données provenant des pays membres d'Interpol et des partenaires du secteur privé.



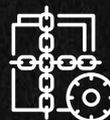
Fraudes en ligne : E-mails et messages de texte truqués prétendant provenir d'une source légitime et utilisés pour induire les personnes à révéler leurs informations personnelles ou financières.



Extorsion numérique : Les victimes sont induites à partager des images sexuellement compromettantes qui sont utilisées aux fins de chantage.



Compromission des courriers électroniques des entreprises : Les criminels piratent les systèmes de courrier électronique pour obtenir des informations sur les systèmes de paiement d'entreprise ; ils induisent ensuite les employés des sociétés à transférer de l'argent dans leur compte bancaire.



Logiciel de rançon : Les cybercriminels bloquent les systèmes informatiques des hôpitaux et des institutions publiques, puis ils exigent de l'argent pour restaurer leur fonctionnalité.



Botnets : Des réseaux d'appareils compromis sont utilisés pour automatiser des attaques cybernétiques à grande échelle.

L'AFRIQUE A DU RETARD POUR RATIFIER LES RÈGLES DE CYBERSECURITE

L'Union africaine a adopté la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, appelée aussi Convention de Malabo, à Malabo (Guinée équatoriale) le 27 juin 2014.

Son objectif est d'établir des règles critiques pour définir un environnement numérique sécuritaire et combler les lacunes dans la réglementation et l'acceptation juridique des communications électroniques et des signatures électroniques. Elle est aussi concernée par l'absence de règles spécifiques qui protègent les consommateurs, les droits de propriété intellectuelle, les données personnelles, les systèmes d'information et le droit à la vie privée en ligne.

Pour le moment, huit pays africains seulement ont ratifié l'accord.

Le Conclave africain sur la sécurité des données précise que les dispositions clés de la Convention de Malabo incluent :

- Définir les règles de sécurité essentielles pour établir un espace numérique crédible pour les transactions électroniques, la protection des données personnelles et la répression de la cybercriminalité.
- Établir une structure juridique visant à renforcer les droits fondamentaux et les libertés publiques, protéger les données physiques et punir toute violation du droit à la vie privée « sans nuire à la libre circulation des données personnelles ».
- Adopter des mesures législatives et/ou réglementaires selon les besoins pour rendre les institutions et leurs responsables spécifiquement responsables en rapport avec leurs réponses aux incidents de cybersécurité.
- Promouvoir la prise de responsabilité en matière de cybersécurité à tous les niveaux du gouvernement en définissant les rôles et responsabilités de façon précise.
- Établir une autorité de protection nationale comme entité administrative indépendante chargée d'assurer que le traitement des données personnelles soit dûment réglementé.
- Développer des partenariats publics/privés comme modèles pour engager l'industrie, la société civile et le secteur académique dans la promotion et l'amélioration d'une culture de cybersécurité.
- Créer des partenariats internationaux visant à réglementer les questions de double responsabilité criminelle, d'échange d'information entre les pays et de réponse aux menaces cybernétiques.

À un niveau plus élémentaire, le réalisme des jeux vidéo modernes est tel que les joueurs axés sur la violence dans le monde réel peuvent exercer en fait leurs tactiques en jouant.

écrasante majorité sont du sexe masculin, démographie cruciale pour les groupes extrémistes.

Le Réseau de sensibilisation à la radicalisation (RAN) déclare que les jeux tels que Call of Duty et Grand Theft Auto permettent aux utilisateurs de créer leurs propres modifications, ce qui peut être abusé par les extrémistes. Le réseau a indiqué : « Cette tactique place des moteurs (de jeu) puissants entre les mains des extrémistes. »

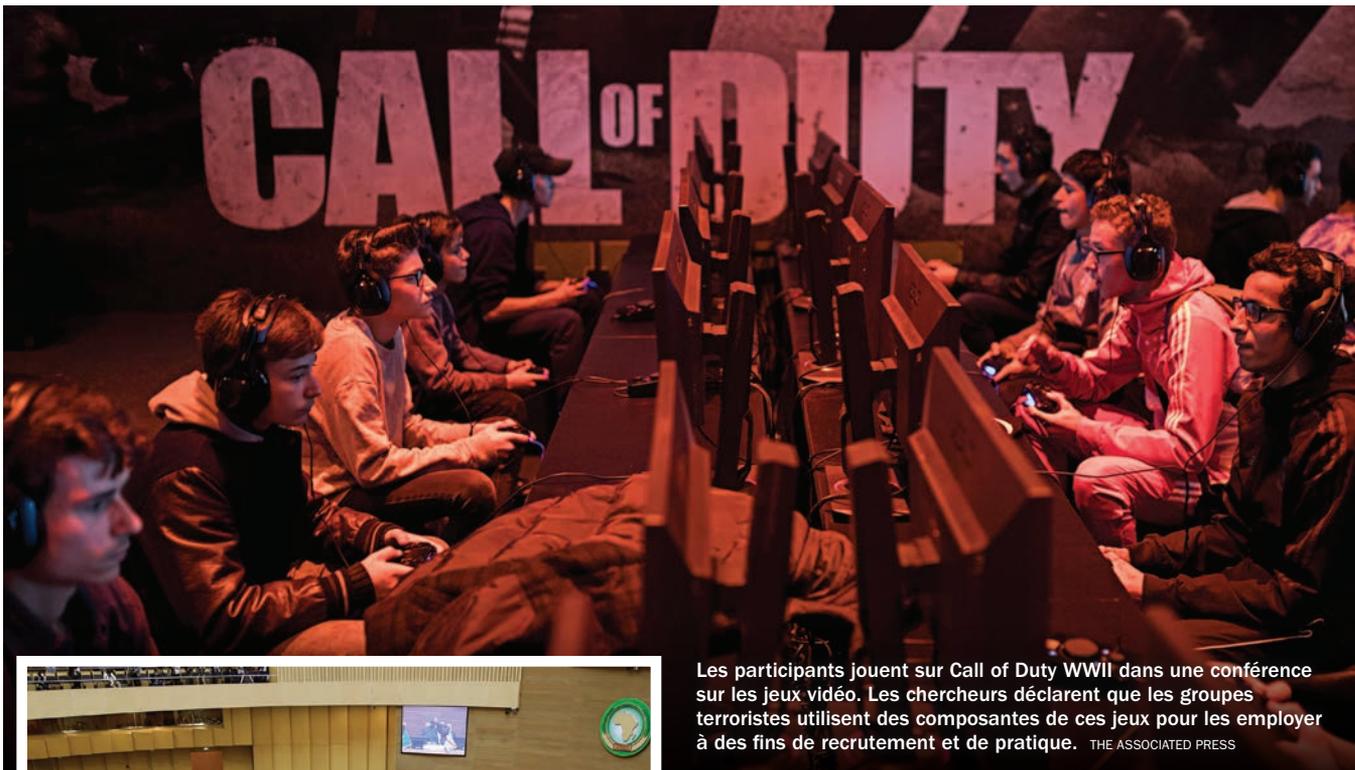
Le RAN a signalé en 2020 : « Les modifications des extrémistes attirent l'attention de la presse et donnent une illusion de crédibilité et de compétence technique aux personnes qui ne sont pas familiarisées avec la manière facile dont ces modifications peuvent être créées. La question de savoir si les jeux modifiés ont jamais eu d'impact sur le recrutement au-delà de la propagande demeure incertaine. »

Un grand nombre de ces jeux réseautés possèdent une fonction de chat qui permet aux joueurs de communiquer entre eux. « Les recruteurs peuvent cibler les gens sur les plateformes ouvertes et commencer à établir des relations avant d'inviter ces personnes dans des environnements plus secrets », déclare le RAN.

À un niveau plus élémentaire, le réalisme des jeux vidéo modernes est tel que les joueurs axés sur la violence dans le monde réel peuvent exercer leurs tactiques en jouant. Le terroriste Anders Breivik qui a tué 77 personnes à Oslo (Norvège) en 2011 s'est entraîné pour ce massacre sur Call of Duty. Dans un manifeste qu'il a écrit, il a appelé Call of Duty: Modern Warfare 2 « probablement le meilleur simulateur militaire qui existe » et a déclaré qu'il considérait le jeu comme « faisant partie de ma simulation de formation ».

UNE PROTECTION EST NÉCESSAIRE

Des recherches indiquent que les gouvernements nationaux doivent être plus proactifs pour se protéger contre les attaques



Les participants jouent sur Call of Duty WWII dans une conférence sur les jeux vidéo. Les chercheurs déclarent que les groupes terroristes utilisent des composants de ces jeux pour les employer à des fins de recrutement et de pratique. THE ASSOCIATED PRESS



Les chefs d'état africains participent à une assemblée de l'Union africaine à Addis-Abeba (Éthiopie) en février 2022.

THE ASSOCIATED PRESS

cybernétiques. Le site web juridique JD Supra indique que, au cours des dix dernières années, 33 pays africains ont promulgué des lois et adopté des règlements sur la cybersécurité, la cybercriminalité, les transactions électroniques et la protection des données.

Les économistes et les professionnels de la technologie ont exhorté les pays africains à ratifier la Convention de Malabo, décrite comme l'un des accords mondiaux les plus élaborés sur la cybersécurité. Son but est d'établir une « structure crédible pour la cybersécurité en Afrique grâce à l'organisation des transactions électroniques, la protection des données personnelles, la promotion de la cybersécurité, l'e-gouvernance et la lutte contre la cybercriminalité ».

Jusqu'à présent, huit pays africains seulement ont ratifié l'accord de Malabo. Pour qu'il entre en vigueur, un minimum de seize pays africains doivent l'adopter.

Le Dr Allen de l'ACSS déclare qu'il n'y a pas suffisamment de professionnels cybernétiques disponibles,

ayant une formation poussée, pour combattre les menaces. Le continent s'empresse de combler son retard.

« Le manque de réponse efficace est dû en partie aux déficits de capacité, écrit le Dr Allen. Le continent fait face à un manque de professionnels certifiés en cybersécurité de 100.000 personnes, chiffre qui est en augmentation. Un grand nombre d'organisations, de commerces et d'agences manquent de sensibilisation cybernétique de base ; ils manquent aussi de mettre en œuvre des mesures de cybersécurité rudimentaires. Les gouvernements échouent fréquemment pour surveiller les menaces, recueillir des preuves forensiques numériques, ou tenter des poursuites relatives à la criminalité informatique. 96 % des incidents de cybersécurité restent non signalés ou non résolus, ce qui veut dire que les menaces cybernétiques en Afrique sont sans doute bien pires que ce qui est reconnu. »

Une préoccupation particulière concerne l'obtention d'un équilibre entre la répression des cybercrimes et des cyberattaques et la préservation des droits humains. Le professeur Boukhars déclare que les cyberterroristes doivent être définis avec « précision » de façon que les droits des citoyens ordinaires ne soient pas limités. Il remarque que les technologies de surveillance sont fréquemment utilisées pour réprimer les dissidents politiques légitimes.

Le professeur Cronin déclare que les gouvernements peuvent « corriger excessivement » en matière de surveillance en espionnant leurs propres citoyens. Un tel espionnage détruit la légitimité du gouvernement et l'état de droit. Elle dit que la légitimité de l'état doit être maintenue en équilibrant la répression des acteurs malveillants et la préservation des droits humains. □



Un luthier autodidacte de la RDC

TRAVAILLE POUR LES STARS

REUTERS

Dans un atelier en tôle d'une ruelle de Kinshasa, capitale de la République démocratique du Congo (RDC), Jean-Luther Misoko Nzalayala, appelé Socklo, taille avec une machette un morceau de bois qui commence à prendre la forme d'un manche de guitare. Il a 61 ans et travaille pieds nus.

Un peu plus tard, il martèlera sur le manche des petits morceaux de plastique blanc provenant d'une chaise pour servir d'incrustation qui guidera la main du guitariste sur la touche, et il utilisera les fils d'un câble de frein de moto comme cordes.

Depuis plus de 40 ans, ce luthier autodidacte emploie une variété de matériaux recyclés et de bois durs locaux pour créer ses guitares. La passion de Socklo a commencé en 1975 dans son village de Kikwit (RDC), lorsqu'il a démonté et copié la guitare qu'un ami lui avait donnée.

Trois ans plus tard, il a déménagé à Kinshasa où il a vendu sa première guitare à un cousin. « Je ne pouvais pas imaginer que les habitants d'une ville comme Kinshasa pouvaient aimer une guitare comme celle-là. Cela m'a donné du courage. »

Il a utilisé les commentaires négatifs pour améliorer

son métier et affiner ses créations. Bientôt, les musiciens locaux et internationaux ont afflué vers son atelier en tôle.

Jupiter Bokondji, vedette de la musique congolaise, a adoré les sons des guitares de Socklo et lui a demandé de fabriquer des guitares électriques. Le résultat, selon Jupiter, est beaucoup plus authentique que les marques majeures de guitare qui coûtent jusqu'à vingt fois plus cher.

« Je l'ai jouée dans le monde entier ; tout le monde est stupéfait, déclare Jupiter. Voir cette guitare faire ce qu'elle fait, la façon dont elle joue, c'est comme une tornade. »

Yarol Poupaud, guitariste français qui a fait plusieurs tournées avec le chanteur de rock Johnny Hallyday pendant des années, a acheté quatre créations de Socklo.

« Elle a de petites imperfections ; elle n'est pas parfaite mais c'est ça qui crée la magie », a-t-il dit en grattant les cordes d'une guitare bleue étoile frappée du drapeau de la RDC.

Le luthier Jean-Luther Misoko Nzalayala, appelé Socklo, joue de la guitare dans son atelier de Kinshasa (République démocratique du Congo).

POUR CONTINUER LA TRADITION, LES ARTISTES SCULPTENT LES OS DE CHAMEAU

REUTERS

L'artisan somalien Muse Mohamud Olosow examine avec soin un énorme amas d'os de chameau jetés par un abattoir de Mogadiscio et sélectionne les pièces qu'il sculptera pour créer des bijoux et des chapelets ornés utilisés par les Musulmans pour réciter des prières,

À sa connaissance, il est l'un de quatre artisans seulement qui travaillent avec les os de chameau, dans un pays de 16 millions d'habitants. Il dit qu'en 1978, pendant l'une des nombreuses périodes de guerre et d'instabilité de Somalie, des tireurs ont tué des douzaines d'artisans à Mogadiscio et dans une autre municipalité.

Pendant des années, il a sculpté ses os en secret chez lui, puis il les amenait aux marchés pour les vendre discrètement.

M. Olosow, qui a des mains fortes et des bras musclés qui présentent des cals à cause de son travail, dit que c'est son père qui lui a enseigné le métier en 1976.

Il prévoit d'assurer que cette tradition vieille de plusieurs décennies ne disparaisse pas avec lui.

Depuis son atelier dans la capitale somalienne, il déclare : « Mes gosses hériteront de moi ces aptitudes que j'ai héritées de mon père. Je ne veux pas que ces aptitudes disparaissent. »

Ses clients sont pour la plupart des officiels de l'état ou des Somaliens riches qui vivent à l'étranger. Un seul chapelet méticuleusement sculpté peut coûter environ 50 dollars, dans un pays où 7 personnes sur 10 vivent avec moins de 2 dollars par jour.

Un client qui s'est rendu dans son atelier déclare que le travail justifie le prix. « Ce qui est important, c'est la qualité, pas le prix. Je préfère celui-ci aux chapelets importés des autres pays comme la Chine. »

Pour M. Olosow et sa famille, la sculpture des os est leur source principale de revenu depuis des décennies. Ils ont investi près de 5.000 dollars pour importer des machines italiennes afin de ciseler et percer ces os durs, dit-il, ce qui est plus rapide et permet de travailler « sans ecchymoses ».

« Notre plan consiste à exporter ces articles dans d'autres pays. Nous continuerons cet artisanat jusqu'à ce que nous devenions riches, si Dieu le veut ! »

L'artisan somalien Muse Mohamud Olosow travaille sur un chapelet orné fabriqué avec des os de chameau mis au rebut, dans son atelier de Mogadiscio. REUTERS



AFP/GETTY IMAGES

— Une star du tennis joue pour — « **MON PAYS, MON CONTINENT, MA RÉGION** »

PERSONNEL D'ADF

La joueuse de tennis tunisienne Ons Jabeur a attiré l'attention du monde entier lorsqu'elle a remporté les internationaux de France de tennis en simple junior en 2011. Aujourd'hui, elle déclare que le tennis est plus qu'un sport pour elle.

La Tunisienne Ons Jabeur réalise un coup droit pendant un tournoi en 2021 aux États-Unis.

Son pays natal a peu d'infrastructure de tennis et n'a aucun moyen établi pour les joueurs qui veulent devenir professionnels. Ons Jabeur dit qu'elle veut changer cela.

Elle a déclaré au journal The National des Émirats arabes unis : « Je ne joue plus pour moi. Je joue pour mon pays, mon continent, ma région. Pour moi, le tennis n'est pas seulement un sport. J'essaie de montrer l'exemple pour ceux qui souhaitent y arriver un jour, ceux qui souhaitent l'opportunité d'entrer en compétition. »

Dès le début 2022, elle est classé 10ème du monde, ce qui en fait le joueur africain de tennis homme ou femme le mieux classé de l'époque.

Elle avait 16 ans lorsqu'elle a gagné la division junior des internationaux de France de tennis, devenant ainsi le premier junior nord-africain à remporter le titre. Depuis lors, sa carrière de joueuse professionnelle de tennis a eu des hauts et des bas. Elle a dû se retirer de l'Open d'Australie en 2022 à cause d'une blessure dorsale. Mais elle s'est fermement établie comme joueuse de premier plan au WTA Tour.

« Je sais qu'il y a beaucoup de femmes dans d'autres pays qui ne peuvent pas faire ça ; en représentant les femmes arabes, je peux montrer l'exemple, dit-elle au National. C'est très important pour moi et j'espère pouvoir réussir à partager ce message. »

Lorsqu'elle était petite en Tunisie, elle n'avait pas parfois accès aux courts de tennis des écoles ou des clubs, ce qui lui forçait de pratiquer sur les courts de tennis des hôtels voisins. Elle a commencé à jouer sur le circuit Junior de la Fédération internationale de tennis en 2007 à l'âge de 13 ans.

Avec ses aptitudes et grâce au soutien de ses parents, elle s'est entraînée en Belgique et en France à partir de 16 ans.

Un hélicoptère de l'unité de sécurité maritime du Nigeria se prépare à secourir des membres dans le cadre d'un exercice anti-piraterie à Lagos. REUTERS



LA PIRATERIE MONDIALE BAISSÉ À SON NIVEAU LE PLUS BAS EN 18 ANS

DEFENCEWEB

En 2021, la piraterie et le vol à main armée en mer ont baissé à leurs niveaux les plus bas en 18 ans. Le Bureau international maritime (BIM) attribue cela à « l'action vigoureuse » des autorités pour protéger les marins.

En 2021, le Centre de reportage de piraterie du BIM a reçu des rapports de 132 incidents de piraterie et de vol à main armée contre des bateaux. 115 vaisseaux ont été abordés, 11 ont été sujets à des tentatives d'attaque, 5 ont essuyé des coups de feu et 1 a été détourné. Le golfe de Guinée reste le point sensible mondial de la piraterie.

Michael Howlett, directeur du BIM, a applaudi la réduction du nombre d'incidents tout en exhortant les états côtiers à suivre étroitement les risques et à affronter « robustement » la criminalité dans leur zone économique exclusive.

« Alors que le BIM applaudit ces actions, il fait aussi appel aux états côtiers du golfe de Guinée pour qu'ils augmentent leur collaboration et leur présence physique dans leurs eaux afin d'assurer une solution à long terme et durable pour faire face aux crimes de piraterie et de vol à

main armée dans la région », a-t-il dit.

La présence en augmentation des vaisseaux navals internationaux et la coopération avec les autorités régionales ont joué un rôle dans cette réduction, selon lui. Ceci a inclus les actions de la Marine royale danoise qui a riposté contre un hors-bord transportant huit pirates présumés en novembre 2021. Quatre ont été tués et les quatre autres capturés.

La région du golfe de Guinée a constaté une baisse des incidents signalés, de 81 en 2020 à 34 en 2021. Les enlèvements en mer ont baissé de 55 % en 2021 dans le golfe. Le golfe de Guinée continue à subir tous les incidents d'enlèvement dans le monde, avec 57 membres d'équipage capturés lors de 7 incidents.

Le Centre de reportage de la piraterie du BIM a averti que la menace pesant sur les marins persiste et il continue d'exhorter les équipages et les navires traversant ces eaux à être prudents. En effet, les contrevenants sont violents et le risque affectant les équipages reste élevé. Une preuve en est l'enlèvement de six membres d'équipage d'un porte-conteneurs à la mi-décembre 2021.

Le Kenya bâtit sa base de données ADN pour stopper la pêche illégale

PERSONNEL D'ADF

Le Kenya bâtit une base de données ADN pour ses espèces marines afin de conserver ses ressources maritimes en présence de la pêche illégale généralisée. L'exercice inclut la collecte des espèces et leur catalogage pour aider le gouvernement à intenter des poursuites pour pêche illégale. Depuis le début du programme en 2022, le Kenya a produit des codes-barres pour environ 115 espèces, y compris des requins, des raies, des crustacés et des mollusques.

Thomas Mkare, scientifique de recherche principal à l'Institut de recherche marine et des pêches du Kenya, a déclaré à l'East African : « Le Kenya a plus de 6.000 espèces commerciales et pendant des années nous ne pouvions pas affirmer que les poissons illégalement capturés provenaient du pays. Avec cet exercice scientifique, nous pourrions prouver nos ressources puisque les poissons, même s'ils se ressemblent physiquement, ont chacun une identification moléculaire spéciale associée à une certaine région. »

Ce projet, qui est anticipé durer plusieurs années, a été lancé lorsque Francis O. Owino, secrétaire principal nouvellement nommé du département d'État des Pêches, de l'Aquaculture et de l'Économie des océans, a exhorté en mars 2021 les scientifiques de l'institut à améliorer la recherche alors que le pays souhaitait stimuler son économie des océans.

M. Owino a déclaré dans un rapport publié par Science Africa : « Le pays exige que vous fournissiez des réponses en tant que chercheurs pour nous faire passer à l'étape suivante. Nous exigeons que vous fournissiez des réponses aux défis de pêche auxquels nous faisons face dans le pays. »

Une fois créée, il est anticipé que la bibliothèque de référence améliorera la sécurité alimentaire en contribuant à une pêche durable. Grâce à la base de données, les poissons vendus n'importe où dans le monde pourront être tracés aux eaux kényanes à l'aide de leurs identifiants uniques d'ADN.

Les ressources marines du Kenya sont en baisse à cause d'un afflux de chalutiers industriels étrangers, notamment ceux venant de Chine. Les analystes déclarent que la pandémie du Covid-19 a aussi incité les gens au chômage à pratiquer la pêche illégale pour gagner de l'argent.

Un rapport compilé par Global Fishing Watch a révélé que 230 chalutiers de pêche étaient actifs au large des côtes du Kenya entre mai et août 2021. Un grand nombre d'entre eux appartenaient à des sociétés chinoises et italiennes, selon Africanews.



AFP/GETTY IMAGES

UN NOUVEAU SYSTÈME DE PAIEMENT AIDE LE COMMERCE INTRA-AFRICAIN

PERSONNEL D'ADF

Un nouveau système aide les détaillants à vendre de l'autre côté de la frontière. Le Système de paiement et de règlement pan-africain (PAPSS) a été lancé à Accra (Ghana) en janvier 2022. Il permet aux acheteurs de payer dans une monnaie nationale de façon que les vendeurs d'un autre pays puissent être payés dans leur propre monnaie locale. Il est conçu pour développer le commerce entre les pays africains et pour traiter les paiements en moins de deux minutes.

« Il y a 42 monnaies en Afrique. Nous voulons nous assurer qu'un marchand du Ghana puisse transférer des cedis ghanéens à un homologue du Kenya, qui recevra des shillings kényans », a déclaré Wamkele Mene, secrétaire général de la zone de libre-échange continentale africaine (ZLECAF), au New Times du Rwanda.

Il a dit que les conversions monétaires africaines peuvent s'élever à 5 milliards de dollars par an. En rationalisant ce processus, le PAPSS peut conserver cet argent sur le continent et pourrait conduire finalement à limiter la dépendance des monnaies étrangères.

Benedict Oramah, président-directeur général de la Banque d'exportation et d'importation d'Afrique (Afreximbank), a posé la question à The Africa Report : « Pourquoi devons-nous demander des devises fortes pour le commerce entre le Kenya et l'Ouganda, ou entre le Sénégal et la Guinée ? Pourquoi ne pouvons-nous pas agir comme si chaque monnaie africaine était convertible en Afrique ? »

Le PAPSS a été développé par l'Afreximbank ; c'est une initiative conjointe qui inclut l'Union africaine et la ZLECAF. L'idée pour le projet remonte à 2016 lorsque les organisateurs ont étudié les systèmes de paiements et les opérateurs en Afrique. L'année suivante, la zone monétaire ouest-africaine a convenu de mettre en œuvre un projet pilote pour servir de démonstration de faisabilité.

L'Afreximbank soutient le système en fournissant des garanties de règlement et des facilités de découvert.

Le programme est entré en vigueur en août 2021 avec des tests de transaction concernant les banques centrales de Gambie, Guinée, Liberia, Nigeria et Sierra Leone. Il a été lancé commercialement en 2022. Le PAPSS a des accords avec douze banques commerciales et quatre commutateurs de paiement.

En plus de réaliser plus facilement des paiements qui franchissent les frontières, le système fait aussi des investissements dans la sécurité en normalisant les systèmes de paiement informels précédents et en mettant en place des protections pour assurer qu'il ne soit pas utilisé par les criminels.

Solomon Quaynor, vice-président de la Banque africaine de développement, a déclaré à The Africa Report : « Le PAPSS comblera le vide qui existe en adaptant les exigences nécessaires concernant la connaissance du client et la lutte contre le blanchiment d'argent au contexte africain. L'infrastructure offerte par le PAPSS améliorera considérablement l'intégration intrarégionale et le commerce intra-africain. »



FORCES ARMÉES DU GHANA

LA MARINE GHANÉENNE AJOUTE QUATRE VAISSEaux POUR SÉCURISER LES CHAMPS DE PÉTROLE OFFSHORE

PERSONNEL D'ADF

La Marine ghanéenne a ajouté quatre nouveaux vaisseaux de sécurité offshore à sa flotte, dans le but de protéger les personnes et les sociétés actives dans sa zone économique exclusive.

Le contre-amiral Issah Adam Yakubu, chef d'état-major de la marine, a reçu les vaisseaux Flex Fighter lors d'une cérémonie au port de Takoradi le 10 janvier 2022. Ces cuirassés de 40 mètres peuvent transporter plus de 70 personnes et une cargaison de 60 tonnes. L'acquisition s'inscrit dans le cadre d'un effort plus vaste pour protéger l'infrastructure pétrolière offshore contre la piraterie.

« Je peux vous assurer qu'au cours des prochains mois nous allons augmenter la surveillance et la vigilance en fonction de cette capacité que nous développons, et nous allons tuer dans l'œuf ce cancer [la criminalité dans le golfe de Guinée] », a déclaré le contre-amiral à My Joy Online.

Au cours des années récentes, les gardes de sécurité privés ont proliféré dans la région pour protéger les structures de pétrole et de gaz offshore. Le journal ghanéen Daily Graphic signale que, à partir de



Le commodore Samuel Walker, officier général du Commandement naval occidental, s'exprime lors d'une cérémonie commémorant l'ajout de quatre nouveaux vaisseaux à la flotte de la Marine ghanéenne. FORCES ARMÉES DU GHANA

2022, seuls les navires de la Marine ghanéenne seront autorisés à protéger ces installations. Tullow Oil et ses partenaires qui exploitent le champ de pétrole Jubilee au large des côtes du Ghana ont signé un protocole d'accord de cinq ans avec la Marine ghanéenne pour assurer la sécurité de l'infrastructure pétrolière et du personnel.

Pendant l'événement, le commodore Samuel Walker, officier général du Commandement naval occidental, a déclaré que les bateaux feront beaucoup pour améliorer la capacité de la Marine ghanéenne à protéger les champs de pétrole et obtenir des revenus pour le pays, selon un reportage du Ghana Peace Journal.

Il a félicité les premiers marins choisis pour être affectés aux vaisseaux et les a exhortés à se maintenir au plus haut degré de professionnalisme et à rester vigilants en ce qui concerne la maintenance des vaisseaux.



LE KENYA VA CONSTRUIRE UN CENTRE CONTRE LES EEI

PERSONNEL D'ADF

Le Kenya construit un centre contre les engins explosifs improvisés (C-EEI) à Embakasi pour lutter contre les menaces extrémistes dans la région.

La nouvelle installation dans l'école de soutien à la paix humanitaire est financée par l'Allemagne et le Royaume-Uni. Depuis 2016, la branche C-EEI a formé plus de 1.700 soldats et policiers provenant du Kenya et de 21 autres pays.

Lors d'une cérémonie pour la pose de la pierre angulaire, les experts des Forces de défense du Kenya (KDF) ont démontré comment détoner en toute sécurité un EEI à l'aide d'un robot télécommandé. Ils ont aussi montré comment une bouteille d'eau peut être utilisée comme engin explosif.

L'ambassadeur adjoint d'Allemagne Thomas Wimmer a déclaré lors de l'événement : « Les EEI sont des tueurs ; non seulement ils tuent les soldats, mais aussi les policiers et les civils. C'est la raison pour laquelle l'Allemagne souhaite financer la branche C-EEI. Elle aide vraiment à empêcher les gens d'être tués, mutilés ou blessés. »

Les EEI sont les armes les plus létales employées par le groupe extrémiste al-Shebab. Entre janvier 2017 et avril 2020, les explosions d'EEI ont tué 153 soldats de la mission de l'Union africaine en Somalie (AMISOM) et 489 membres des forces de sécurité somaliennes. Des soldats du Kenya participent à l'AMISOM.

« Ces engins représentent la plus grande menace pesant sur les KDF et les soldats des autres pays contributeurs qui combattent al-Shebab dans le cadre de la mission de l'Union africaine en Somalie », a déclaré Josephine Gauld, haute-commissaire adjointe britannique au Kenya, pendant la cérémonie.

Elle a dit que le centre C-EEI fait partie d'un centre d'excellence en développement à Embakasi, où les forces armées de la région peuvent apprendre les techniques nécessaires pour contrer toute une série de menaces.

« L'école de soutien à la paix humanitaire est une initiative unique sur le continent africain, qui fournit une fondation solide sur laquelle construire un centre d'excellence régional compétent et capable où le personnel policier et militaire d'Afrique de l'Est et d'Afrique australe reçoit une formation d'élimination des EEI qui aide à améliorer la sécurité et la stabilité en Somalie. »

La première phase de construction coûtera environ 2,6 millions de dollars et inclura 12 bâtiments.

Un soldat des Forces de défense du Kenya démontre des techniques lors d'un événement commémorant la construction d'un nouveau centre pour former les forces de sécurité afin de détecter et désarmer les explosifs improvisés.

FORCES DE DÉFENSE DU KENYA

UN ÉVÉNEMENT CIVILO-MILITAIRE OFFRE DES SOINS VÉTÉRINAIRES GRATUITS

PERSONNEL D'ADF

Pendant trois jours en février 2022, les bergers du Sud-Ouest du Niger ont amené leur bétail et autres animaux pour recevoir des soins vétérinaires indispensables à l'occasion d'un événement gratuit.

Pendant cet événement à Gaya, des vétérinaires ont traité plus de 13.000 animaux avec des vaccins et des vitamines. Les organisateurs ont aussi distribué des radios portables fonctionnant sur l'énergie solaire, qui permettent aux bergers de suivre la météo et les développements sécuritaires dans la région.

Cet événement est l'un des nombreux organisés par la division ACM (action civile-militaire) des Forces armées nigériennes (FAN), dont le but consiste à soutenir les communautés vulnérables et à développer la confiance entre l'armée et les civils.

L'unité ACM de la base aérienne 101 de Niamey a organisé l'événement vétérinaire avec le soutien des soldats américains des affaires civiles affectés à la base. Des événements similaires ont été organisés près de la base aérienne 201 d'Agadez.



Un éleveur de bétail nigérien montre un certificat de « bétail sain » après un événement vétérinaire gratuit à Gaya organisé par la division ACM (action civile-militaire) des Forces armées nigériennes. AMBASSADE DES ÉTATS-UNIS AU NIGER

Le capitaine Badagé Oumarou, commandant de la base aérienne 201, a déclaré en 2021 à la suite d'un événement où les soldats ont distribué du riz, des ballons de foot et des tapis de prière : « Les différentes actions des forces de défense et de sécurité et des partenaires américains sont vraiment appréciées par la population locale. Les habitants de Teghazert ont montré leur gratitude et nous ont exhortés à développer et continuer cet effort. »

Pendant sa première année, l'unité ACM d'Agadez a conduit 11 missions d'assistance dans la région, en aidant un nombre de résidents estimé à 4.200 avec des aliments de base et des fournitures sanitaires pour les protéger contre le Covid-19.

« Les donations telles que celle-ci montrent la valeur à long terme des efforts conduits par FAN/ACM, en particulier lorsque l'unité continue à augmenter sa portée et à servir davantage de communautés », a déclaré le sergent Joseph Bovee des affaires civiles des États-Unis.

Le Malawi lance son programme de moustiquaires

PERSONNEL D'ADF

Le Malawi a commencé la distribution générale des moustiquaires au plus grand nombre possible de personnes parmi ses 19 millions d'habitants.

Les moustiquaires réduisent la propagation du paludisme, qui est responsable pour 36 % de toutes les visites d'hôpital en consultation externe et 15 % des hospitalisations au Malawi.

Khumbize Kandodo Chiponda, ministre de la Santé du Malawi, a annoncé la campagne soutenue par le Fonds mondial lors de la commémoration de la Journée du paludisme de la Communauté de développement d'Afrique australe. Elle a déclaré au Nyasa Times qu'elle espérait que les 9 millions de moustiquaires du programme seraient utilisées chacune par deux personnes partageant une même zone ou lit à moustiquaire.

Elle a aussi dit que les agents de santé donneraient des médicaments antipaludéens à toutes les femmes enceintes pour empêcher qu'elles ne souffrent de la maladie pendant leur grossesse.

Le paludisme est la maladie la plus meurtrière du Malawi. En 2020, il y a provoqué la mort de 2.500 personnes : c'est



©UNICEF/MALAWI/ATLAS MEDIA

plus que toute autre maladie, y compris le Covid-19.

Mme Chiponda a déclaré que la campagne affrontait des défis majeurs.

« Et l'un de ces défis est le fait que, lorsque vous distribuez des moustiquaires, en particulier près d'un lac, vous constatez que ces moustiquaires sont utilisées pour la pêche et d'autres choses », a-t-elle dit à Voice of America.

Pour réduire la possibilité d'un tel usage abusif, la campagne inclut aussi l'enseignement aux bénéficiaires de l'importance de dormir sous la moustiquaire.

Mme Chiponda a déclaré au Nyasa Times : « L'Afrique dépense environ 12 milliards de dollars annuellement pour le paludisme. Il y a 400.000 décès annuels dus au paludisme dans la région de la CDAA [Communauté de développement d'Afrique australe]. Donc, les états membres de la CDAA œuvrent ensemble pour s'assurer que nous affrontons directement le paludisme. »

Un nouveau test de drogue offre l'espoir à des millions

REUTERS

La version révisée d'un médicament reconnu contre la bilharziose, maladie tropicale provoquée par un vers parasitaire, s'est avérée efficace chez les enfants d'âge préscolaire. Il est probable qu'elle offrira un traitement à des millions de personnes.

La société chimique allemande Merck KGaA a signalé que, lors d'essais en phase avancée en Côte d'Ivoire et au Kenya sur des enfants infectés entre 3 mois et 6 ans, plus de 90 % des participants n'avaient plus d'œufs de parasite dans leurs selles ou leur urine après trois semaines ou moins de traitement.

La société déclare qu'elle va maintenant faire une demande d'approbation auprès des organismes de réglementation pour produire et

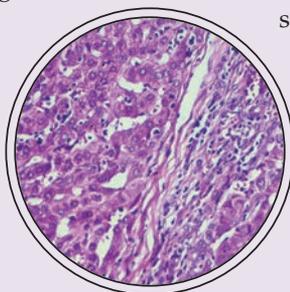
distribuer ce médicament par voie orale. L'arpraziquantel est une version pédiatrique expérimentale du praziquantel standard.

Merck dit qu'il s'est aussi avéré sûr et bien toléré.

Le Consortium pédiatrique du praziquantel a confirmé les résultats positifs et déclaré que la bilharziose est l'une des maladies parasitaires qui causent le plus de dommages dans le monde. L'Organisation mondiale de la santé signale que 105,4 millions de personnes étaient traitées pour la maladie en 2019.

Le praziquantel est le traitement standard pour les écoliers et les adultes, ce qui laisse un nombre de nourrissons et d'enfants préscolaires estimé à 50 millions sans option de traitement.

La maladie, appelée aussi schistosomiase, est provoquée par des plathelminthes parasites. Elle se propage par l'intermédiaire d'escargots d'eau douce dans les régions tropicales et subtropicales de la planète, mais elle affecte surtout les communautés pauvres et rurales de l'Afrique subsaharienne.



Échantillon de pathologie humaine de bilharziose sous microscope

L'aube de l'humanité est reculée de 30.000 ans

PERSONNEL D'ADF

L'âge des plus anciens fossiles d'Afrique de l'Est reconnus généralement comme représentant l'espèce humaine est incertain depuis longtemps. Maintenant, la datation d'une énorme éruption volcanique dans le Sud-Ouest de l'Éthiopie révèle que certains fossiles sont bien plus anciens qu'on ne pensait précédemment.

Les scientifiques ont découvert des restes appelés Homme de Kibish en Éthiopie vers la fin des années soixante, selon un reportage dans SciTechDaily. Depuis, ils essaient de les dater avec précision en utilisant les empreintes chimiques des niveaux de cendre volcanique trouvés au-dessus et au-dessous des sédiments où les fossiles ont été découverts.

Une équipe internationale de scientifiques conduite par l'Université de Cambridge a maintenant réévalué l'âge de l'Homme de Kibish et des êtres humains (Homo sapiens) en tant qu'espèce. Une datation précédente des fossiles leur avait donné un âge de moins de 200.000 ans, mais la nouvelle recherche montre qu'ils

doivent être plus anciens qu'une éruption volcanique colossale qui s'était produite il y a 230.000 ans. Les résultats ont été rapportés dans le journal Nature.

Le professeur Asfawossen Asrat de l'université d'Addis-Abeba a fait la déclaration suivante, selon le rapport de l'Université de Cambridge : « La formation Omo Kibish est un vaste dépôt sédimentaire qui a été peu accédé et investigué auparavant. Notre étude plus approfondie de la stratigraphie [l'ordre et la position des strates des restes archéologiques] de la formation Omo Kibish, en particulier les strates de cendre, nous ont permis de reculer l'âge du plus ancien Homo sapiens dans la région à au moins 230.000 ans. »

Cette région d'Éthiopie a de longs antécédents de forte activité volcanique et est une source des premiers restes d'êtres humains et d'artéfacts tels que les outils de pierre.

Le Dr Aurélien Mounier du musée de l'Homme de Paris a indiqué dans l'étude : « Omo I possède des caractéristiques humaines modernes catégoriques, par exemple une voûte crânienne haute et globulaire et un menton. La nouvelle estimation de date en fait ainsi le plus ancien Homo sapiens incontesté en Afrique. »

Les scientifiques ont mis à niveau leurs recherches sur les fossiles humains trouvés dans la formation Omo Kibish au Sud-Ouest de l'Éthiopie.

PHOTO PAR JOHN FLEAGLE/NATIONAL SCIENCE FOUNDATION



La Somalie ouvre un centre pour surveiller les locustes

PERSONNEL D'ADF

Depuis la fin 2019, la région de la Corne de l'Afrique au sens large est en proie à la pire invasion de criquets pèlerins depuis des décennies. Maintenant, la Somalie a ouvert un centre de détection des locustes pour aider à affronter la crise.

Les locustes ont détruit des dizaines de milliers d'hectares de récoltes et de pâturage. En Somalie où la majorité des habitants dépendent de l'agriculture et de l'élevage comme moyens de subsistance, la sécheresse et les inondations périodiques ont érodé fortement la sécurité alimentaire des ménages. La crise des criquets pèlerins a simplement rendu la vie plus difficile.

La Somalie, ainsi que l'Organisation des Nations unies pour l'alimentation et l'agriculture, ont ouvert le Centre national de surveillance et de contrôle des criquets pèlerins basé à Qardho dans la région Nord-Est du pays.



AFP/GETTY IMAGES

Said Hussein lid, ministre somalien de l'Agriculture et de l'Irrigation, a déclaré que le gouvernement avait fait du contrôle des criquets pèlerins et autres espèces invasives une priorité et qu'il promulguait des lois pour protéger le pays contre de telles invasions, selon un reportage de Hiiraan News de Somalie. Le centre de surveillance sera une source majeure d'information sur les invasions de locustes dans la région.

L'ONU a déclaré que la Somalie avait enregistré des gains majeurs en supprimant l'un des plus grands afflux de criquets pèlerins dans l'histoire récente.

Les criquets pèlerins peuvent gravement endommager les récoltes parce que les insectes sont résilients, très mobiles et se nourrissent d'une grande quantité de toute sorte de végétation, y compris les récoltes, les pâturages et le fourrage des bovins.

Un essaim peut être typiquement constitué de plusieurs centaines de millions de locustes au km carré. Ils s'envolent en suivant les vents, et peuvent se déplacer jusqu'à 150 km par jour. Ils peuvent facilement manger une quantité de végétation égale à leur propre poids chaque jour.



Le Bénin est désigné comme endroit où les affaires démarrent le plus vite

PERSONNEL D'ADF

Antérieurement, le Bénin était peut-être connu au mieux pour ses exportations de coton et ses créations de vêtements aux couleurs vives. Mais aujourd'hui, il est connu pour sa bureaucratie rationalisée, qui permet aux nouvelles entreprises de s'établir plus rapidement que dans n'importe quel autre pays africain.

En fournissant un service en ligne complet, le gouvernement a aidé les entrepreneurs à créer des entreprises et des emplois pendant la pandémie du Covid-19. Le tiers des nouveaux entrepreneurs béninois sont des femmes, selon les Nations unies.

Un rapport de l'ONU décrit comment Sandra Idossou, femme d'affaires béninoise, a ouvert une boutique d'artisanat à Cotonou, la capitale commerciale du pays. Avec les restrictions du Covid-19 en vigueur et mises en application par les autorités, elle a utilisé son

smartphone pour se connecter au site web d'enregistrement des nouvelles sociétés du Bénin. En moins de dix minutes, elle avait saisi ses informations, photographié et téléchargé ses pièces d'identité, et payé par carte de crédit.

Deux heures plus tard, elle a reçu un e-mail avec ses certificats de constitution en société et son entreprise a été officiellement créée.

Sa boutique appelée Kouleurs d'Afrik vend maintenant des articles faits à la main à partir de matériaux jetés, trouvés en ville. Sandra Idossou a déclaré à Voice of America : « Sans cette facilité avec laquelle on peut créer une affaire en ligne, s'il fallait faire la queue, attendre, parcourir un labyrinthe administratif pour démarrer une entreprise, je ne l'aurais jamais fait. C'est aussi simple que cela. Je serais restée dans le secteur informel. »

Une plateforme gouvernementale numérique de l'ONU appelée eRegistrations place le Bénin et l'Estonie comme les pays du monde où on peut démarrer le plus rapidement une entreprise. Le temps de démarrage moyen est de trois jours dans l'Union européenne et sept jours à New York.

Le programme eRegistrations fonctionne dans d'autres pays en développement, y compris le Lesotho et le Mali. La plateforme permet aux procédures officielles d'être accessibles et transparentes, en particulier pour les petites entreprises. Les procédures administratives sur papier sont caractérisées dans le monde entier par de longues files à l'extérieur des bureaux du gouvernement et plusieurs heures de bureaucratie. Ces procédures peuvent aussi nécessiter de se rendre dans différents bureaux du gouvernement utilisant des formulaires presque identiques.

Les taxis africains deviennent verts

REUTERS

À la fin 2021, le service de parc de taxis électriques Nopea Ride a ouvert au Kenya un centre de charge des véhicules électriques (VE) à Village Market dans la capitale de Nairobi, montrant ainsi une hausse de la demande pour la mobilité électrique en Afrique de l'Est.

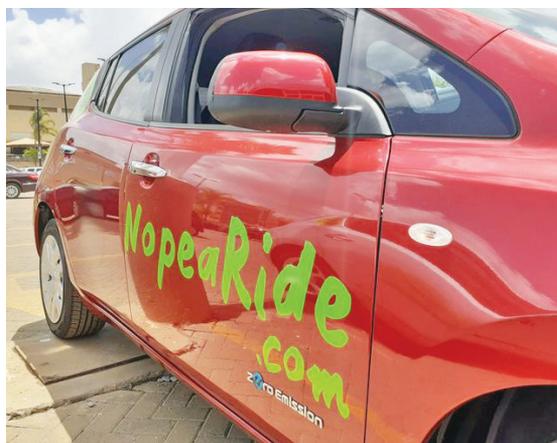
Cette société finlandaise de taxis électriques avait précédemment annoncé qu'elle prévoyait de tripler son parc de Nairobi, ce qui aiderait à réduire les émissions du trafic notoire de la ville. EkoRent, société-mère de Nopea, a maintenant un parc d'environ 1.500 VE.

La société estonienne Bolt de transport sur demande a annoncé en octobre 2021 qu'elle inaugurerait des taxis électriques en Afrique du Sud. L'annonce a été faite quatre mois après l'introduction par la société de services de livraison alimentaire par vélo électrique dans ce pays.

« Nous espérons inaugurer une catégorie de taxis verts en Afrique du Sud au cours des prochains mois, et nous projetons d'inaugurer des catégories vertes dans d'autres marchés africains », a déclaré Paddy Partridge, directeur régional de Bolt pour l'Afrique et le Moyen-Orient.

Les VE ont une raison d'être économique en Afrique, en particulier au Kenya où les prix du carburant fluctuent sans avertissement. Les chauffeurs de taxi et les propriétaires de véhicule électrique ou hybride ont de meilleures marges de bénéfice et des intervalles d'entretien plus longs.

En mai 2020, Vaya Africa, entreprise de mobilité avec service de taxis en ligne fondée par le magnat zimbabwéen Strive Masiyiwa, a dévoilé un service de taxis électriques et un réseau de charge au Zimbabwe, avec des plans d'expansion sur le continent.



LES PNEUS USÉS SONT DE L'OR NOIR

REUTERS

Au Nigeria, qui dépend fortement des revenus de ses exportations de pétrole, l'entrepreneuse Ifedolapo Runsewe a identifié un autre type d'or noir : les pneus usés des voitures.

Elle a créé Freetown Waste Management Recycle, usine industrielle engagée dans la transformation des vieux pneus en briques de pavement, carreaux de plancher et autres articles qui font l'objet d'une forte demande.

« Créer quelque chose de nouveau à partir de quelque chose qui serait jeté quelque part comme déchet faisait partie de ma motivation », dit-elle dans son usine d'Ibadan. « Nous sommes capables de créer une chaîne complète de valeur avec les pneus », déclare-t-elle en saisissant une brique de pavement, l'un des articles les plus vendus de la société.

La gestion des déchets au Nigeria est au mieux sporadique. Dans les villages, les municipalités et les villes, les amas de déchets sont fréquents et les résidents brûlent souvent les déchets pendant la nuit dans l'absence d'une méthode d'élimination plus sûre. Les pneus sont généralement jetés et abandonnés.

Freetown emploie des ramasseurs qui recueillent les vieux pneus dans les décharges. Ils reçoivent 70 à 100 nairas (17 à 24 cents) le pneu. Certains pneus sont fournis directement par des mécaniciens tels qu'Akeem Rasaq, qui est ravi d'avoir trouvé un lieu où il peut gagner un peu d'argent avec ses vieux pneus.

« La plupart des pneus finissent par boucher les drains publics, mais les choses ont changé », dit-il dans son atelier du bord de route.

Freetown a commencé ses opérations en 2020 avec quatre employés seulement. La croissance a été si rapide que les effectifs ont grimpé à 128. Jusqu'à présent, plus de 100.000 pneus ont été recyclés sous forme de matériau pour les ralentisseurs de route ou le pavage souple des terrains de jeu.

Un homme organise des carreaux emboîtés en caoutchouc fabriqués à partir de pneus de voiture recyclés à l'usine de Freetown Waste Management Recycle à Ibadan (Nigeria). REUTERS



LES GUERRIÈRES DU DAHOMEY

TROPENMUSEUM/WIKIMEDIA COMMONS

PERSONNEL D'ADF

En 1861, 3.000 femmes soldats lourdement armées chargent une muraille d'épines pour démontrer leurs aptitudes.

Leur souverain, le roi Gléglé du Dahomey (région qui fait aujourd'hui partie du Bénin), souhaite vivement démontrer la férocité et la compétence de ses guerrières. La muraille de 400 mètres de long est truffée de branches d'acacia avec des épines pointues de 5 cm de long.

Les femmes vont pieds nus, armées de massues et de couteaux. Certaines d'entre elles, les « faucheuses », ont des rasoirs d'un mètre de long qui, selon le roi, pourrait couper un homme en deux.

Les guerrières chargent la muraille en ignorant les blessures sauvages causées par les épines. Elles réussissent à monter au sommet en simulant des combats rapprochés avec un ennemi invisible. Elles descendent, puis elles remontent la muraille une deuxième fois, cette fois en sauvant une bande de villageois jouant le rôle de prisonniers.

La démonstration prouve aux visiteurs que les femmes ne sont pas seulement des personnages de cérémonie. Elles sont en fait les seules femmes soldats du monde affectées aux combats à l'époque.

Il est probable que les guerrières du Dahomey sont apparues au dix-septième siècle. Selon une théorie, elles ont commencé comme chasseuses dans la tribu des Fons. Toutefois, Stanley Alpern, chef de file des experts sur ces guerrières, écrit dans son livre de 1998 intitulé « Les Amazones de la Sparte noire » qu'elles ont probablement commencé en tant que gardes du palais dans les années 1720. Elles ont fini par être appelées « Mino », ce qui veut dire « Nos mères » dans la langue fon.

Ces femmes du Dahomey ont participé à de nombreuses batailles. M. Alpern déclare que, au cours de quatre campagnes majeures vers la fin du dix-neuvième siècle, au moins 6.000 et jusqu'à 15.000

d'entre elles ont trouvé la mort au combat.

Il existe plusieurs théories sur les raisons pour l'existence des guerrières du Dahomey, mais on pense généralement que c'était une question de nécessité : les hommes de la tribu, à cause des guerres et de la traite des esclaves, étaient inférieurs en nombre, dans un rapport de 10 contre 1, comparé à leurs rivaux de la tribu des Yorubas. De ce fait, les femmes ont été recrutées pour se battre.

Il y avait seulement 600 guerrières dahoméennes environ jusque vers le milieu du dix-neuvième siècle, lorsque le roi Ghézo a augmenté leur nombre à environ 6.000. Il est probable qu'il a pu recruter un grand nombre de femmes pour vivre comme guerrières parce que les Dahoméennes de l'époque vivaient dans la pauvreté et étaient souvent maltraitées.

En tant que guerrières, les femmes ont vécu dans le périmètre royal. L'explorateur Richard Burton a précisé que les femmes recevaient des aliments, du tabac, de l'alcool et des esclaves.

Les guerrières étaient entraînées de façon intensive pour se battre, supporter de grandes souffrances et survivre. Les observateurs disaient que, bien qu'elles soient inaptes aux armes à feu, elles étaient expertes dans les combats rapprochés et l'emploi des couteaux.

Jusqu'au début du vingtième siècle, ces femmes ont été dans un état de guerre constante sur la demande de leurs rois ambitieux. Mais lorsque les Français ont envahi avec des armes modernes, les femmes ont été vaincues et leurs groupes ont été dissouts.

Leur bravoure est résumée dans un credo que les femmes répétaient apparemment pour démontrer leur esprit : « Celles qui reviennent de la guerre sans avoir conquis doivent mourir. Si nous battons en retraite, notre vie est à la merci du roi. Nous devons vaincre toute ville qui doit être attaquée, sinon nous nous enterrerons dans ses ruines. »



INDICES

- 1 Les êtres humains pêchent et chassent dans cette région depuis 2.000 ans. Ils ont créé des monticules de fruits de mer, certains avec une longueur de plusieurs centaines de mètres.
- 2 Certains monticules contiennent des lieux de sépulture.
- 3 Cette zone s'est formée à l'intérieur du delta de trois rivières.
- 4 Elle inclut 200 îles et îlots, des forêts de mangroves et un mélange d'eau de mer et d'eau douce.

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.

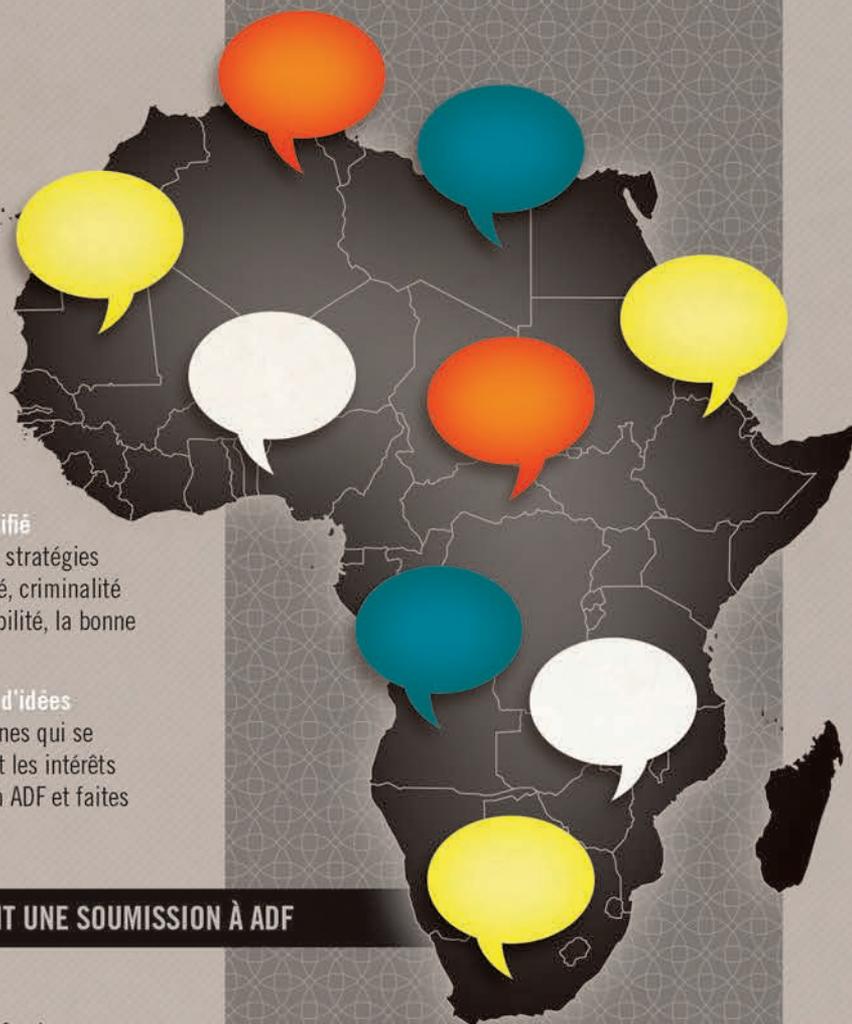
DROITS D'AUTEUR Les auteurs conservent les droits à leur texte original. Cependant, nous nous réservons le droit de revoir et corriger les articles pour qu'ils soient conformes au style de l'Associated Press et s'intègrent dans l'espace disponible. Le fait de soumettre un article ne garantit pas sa publication.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



Vous êtes impatient de lire le prochain numéro ?

À ADF-Magazine.com, nous vous offrons chaque semaine un traitement en profondeur des enjeux actuels qui affectent la paix et la stabilité. Consultez notre site web pour les mêmes actualités crédibles et précises sur la sécurité, sur une base hebdomadaire, provenant de tout le continent.



RESTEZ CONNECTÉ

Si vous souhaitez rester branché sur les réseaux sociaux, suivez ADF sur Facebook, Twitter et Instagram. Vous pouvez aussi vous abonner à notre liste de diffusion électronique en vous inscrivant sur notre site Web, ADF-Magazine.com, ou en envoyant un courriel à News@ADF-Magazine.com.

