NTIS/002/2014

Nations Unies
Commission économique pour l'Afrique

# Note d'orientation

## Relever les défis de la cybersécurité en Afrique

### 1. Introduction

Le Rapport économique sur l'Afrique (2013), publication conjointe de la Commission économique pour l'Afrique (CEA) et de la Commission de l'Union africaine (CUA), indique qu'« après deux décennies de quasi-stagnation, la croissance de l'Afrique s'est sensiblement améliorée depuis le début du XXIe siècle[1]. » Depuis 2000, le continent africain connaît une envolée prolongée des cours des produits de base et une croissance soutenue. Le rapport indique en outre que « compte tenu d'une prévision de 4,8 % en 2013 et de 5,1 % en 2014, par exemple, les perspectives de croissance à long terme de l'Afrique demeurent fermes[2]. » Il convient également de noter que des publications aussi prestigieuses que The Economist[3] et l'International Business Times[4] et des organisations comme la Banque africaine de développement (BAD)[5] ont affirmé que l'Afrique abrite certaines des économies à la croissance la plus rapide au monde.

Cette nouvelle Afrique, symbolisée par la formule « L'Afrique se lève », trouve son expression dans le développement de sa classe moyenne et dans l'adoption rapide de la téléphonie mobile. Selon des estimations récentes de l'Union internationale des télécommunications (UIT), le taux d'abonnement aux services mobiles atteignait 63% en 2013 et plus de 16% de la population africaine utilisent maintenant l'Internet[6]. En outre, on estime que la valeur globale des ventes au détail par Internet s'élevait en 2013 à 963 milliards de dollars[7] alors que, pendant la même période, le commerce électronique entre entreprise et consommateur s'élevait à 1 300 milliards de dollars[8]. Bien que le

1 Commission de l'Union africaine et Commission économique pour l'Afrique, *Tirer le plus grand profit des produits de base africains: l'industrialisation au service de la croissance, de l'emploi et de la transformation économique, 2013,* (publication de l'ONU), référence: F.13. IIK.1.

2 Ibid.

3 J. O'S, "Growth and other good things", The Economist, 1er mai 2013. Disponible à l'adresse www.economist.com/ blogs/baobab/2013/05/ development-africa.

4 Mike Obel, "Africa poised for unprecedented, long-term economic growth: Seven drivers that could transform Africa into the world's economic powerhouse", International Business Times, 13 septembre 2013. Disponible à l'adresse www.ibtimes.com/africa-poised-unprecedented-long-term-economic-growth-seven-drivers-could-transform-africa-worlds.

5 Groupe de la Banque africaine de développement, «Africa is now the fastest growing continent in the world», 7 novembre 2013. Disponible à l'adresse www.afdb.org/en/news-and-events/article/africa-is-now-the-fastest-growing-continent-in-the-world-12107/.

6 Union internationale des télécommunications, «Données et chiffres concernant les TIC», UIT Bureau de développement des télécommunications (Genève, 2008). Disponible à l'adresse www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf.

7 Goldman Sachs, "eCommerce expected to accelerate globally in 2014", Equity Research, New York: The Goldman Sachs Group, Inc., 5 mars 2013. Disponible à l'adresse http://boletines.prisadigital.com/Global_ecommerce.pdf.

8 eMarketer, "eMarketer in review – key 2013 trends, coverage areas and platform growth", Newsroom, 4 septembre 2013. Disponible à l'adresse www.emarketer.com/newsroom/index.php/emarketer-review-key-2013-trends-coverage-areas-platform-growth/#UG1Ch9mS5hMlp1JX.99.

marché du commerce électronique soit dominé par les pays développés, on s'attend à ce que la part globale du commerce électronique au Moyen-Orient et en Afrique passe de 1,6% en 2011 à 2,3% en 2016.

Cependant, de nouveaux défis se posent parallèlement à la croissance, et l'augmentation de l'utilisation des technologies présente ses propres vulnérabilités et risques. L'un de ces risques, qui découle de l'augmentation de l'utilisation des technologies et nécessite une attention et des mesures urgentes, est la cybercriminalité[9].

La cybercriminalité est un phénomène mondial en pleine croissance qui, selon un rapport publié par Symantec Corporation[10] en 2013, augmente plus rapidement en Afrique que dans toute autre région du monde. En effet, les experts de la cybersécurité estiment que, sur le continent africain, 80% des ordinateurs personnels sont infectés par des virus et autres logiciels malveillants[11].

Les cybercriminels ont longtemps considéré l'Afrique comme un lieu providentiel pour commettre leurs actes criminels. Les statistiques provenant de diverses sources indiquent que l'Afrique est très vulnérable aux cybermenaces en raison du nombre élevé de domaines à faible sécurité des réseaux et de l'information. Par exemple, selon la Rapport Norton sur la cybercriminalité, chaque seconde, 18 adultes sont victimes de la cybercriminalité, soit plus de 1,5 million de victimes dans le monde par jour. En outre, l'Afrique du Sud (80%) enregistre le troisième plus grand nombre de victimes de la cybercriminalité dans le monde, après la Russie (92%) et la Chine (84%[12]).

Le rapport Symantec[10] révèle en outre qu'en 2012, le nombre de cyberattaques ciblées en Afrique a augmenté de 42% alors que 31% de ces attaques, qualifiées de cyberespionnage, ont frappé les grandes et les petites entreprises. Les particuliers sont également devenus vulnérables aux virus et autres formes de cybermenaces. En Afrique, le Nigéria est la plus grande source et la première cible des activités Internet malveillantes et les conséquences de cet état de fait se font malheureusement sentir dans les autres pays de la sous-région ouest-africaine. Dans les grandes villes africaines, comme Le Caire, Johannesburg, Lagos et Nairobi, le taux des délits liés à Internet, comme les transactions financières frauduleuses et les enlèvements d'enfants, en particulier au Kenya, a doublé au cours des trois dernières années.

La récente utilisation des technologies de l'information et des communications (TIC) pour faciliter les attaques terroristes en Afrique ajoute une dimension supplémentaire à la question de la cybersécurité. Les données recueillies lors de l'enquête sur l'attaque récente du centre commercial Westgate au Kenya, et les activités de Boko Haram au Nigéria et d'Al-Qaida au Maghreb islamique (AQMI) en Afrique du Nord mettent en évidence l'utilisation des TIC dans la planification, la coordination et la mise en œuvre de ces attaques ainsi que dans leur retentissement médiatique. Ces attaques ont déstabilisé et entravé la récente croissance économique des pays africains. Par exemple, l'attaque du centre commercial Westgate a non seulement coûté au moins 67 vies innocentes et des millions de dollars de dégâts sur les infrastructures, mais on estime qu'elle aura coûté à l'économie kenyane quelque 200 millions de dollars en pertes de recettes touristiques[13].

Par conséquent, les pays africains doivent intensifier de toute urgence les efforts qu'ils déploient contre la cybercriminalité, au moyen d'une approche multipartite incluant les

9 La cybercriminalité est définie comme un vaste ensemble d'activités illégales commises au moyen ou par l'intermédiaire d'un système ou d'un réseau informatique, y compris les délits comme la possession et l'offre ou la diffusion illégales d'informations au moyen d'un système ou d'un réseau informatique.

10 Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18, avril 2013. Disponible à l'adresse www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

11 Franz-Stefan Gacy, "Foreign policy: Africa's internet threat", National Public Radio, 29 mars 2010. Disponible à l'adresse www.npr.org/templates/story/story.php?storyId=125297426.

12 Symantec Corporation, *2012 Norton Cybercrime Report*, septembre 2012.

13 Jacob Kushner, Jacob, "Mall terrorist attack may cost Kenya $200 million in lost tourism earnings", The Associated Press, 1er octobre 2013. Disponible à l'adresse www.ctvnews.ca/mall-terrorist-attack-may-cost-kenya-200-million-in-lost-tourism-earnings-1.1478573.

pouvoirs publics, l'industrie et les organisations de la société civile.

Conformément à la nouvelle orientation stratégique de la CEA sur les stratégies fondées sur les faits et la recherche analytique, la présente synthèse contient des options visant à endiguer les menaces pour la sécurité économique nationale posées par la cybercriminalité et les cybercriminels, que les États membres devront examiner dans le cadre de la Convention de l'Union africaine sur la sécurité du cyberespace et la protection des données personnelles.

## 2. L'impact économique de la cybersécurité

L'absence de cybersécurité a des conséquences économiques colossales. Le rapport Norton sur la cybercriminalité (2012) indiquait que les pertes financières directes s'établissaient en moyenne à 197 dollars par victime dans le monde, et que des pertes financières directes de 110 milliards de dollars avaient été enregistrées dans le monde[14].

Une étude récente d'International Data Group Connect[15] sur l'état des cybermenaces dans différentes régions d'Afrique, plus particulièrement centrée sur l'Égypte, le Kenya, le Nigéria et l'Afrique du Sud, montre qu'il existe une forte corrélation entre la cybersécurité et la croissance économique.

Traditionnellement, l'Afrique a un taux élevé de piratage de logiciels. Selon une étude de 2011[16], le taux moyen de piratage de logiciels dans la région est d'environ 73%; il a peu évolué au cours des dernières années. Outre les pertes financières (1,785 milliards de dollars), le niveau élevé d'utilisation de logiciels non autorisés est susceptible d'aggraver les problèmes causés par les virus et les logiciels malveillants.

Selon l'étude d'International Data Group Connect, chaque année, la cybercriminalité coûte 573 millions de dollars à l'économie sud-africaine, 200 millions de dollars à l'économie nigériane et 36 millions de dollars à l'économie kenyane[15].

Une étude de 2011 de Deloitte Touche indiquait que les institutions financières du Kenya, du Rwanda, de l'Ouganda, de la République-Unie de Tanzanie et de la Zambie avaient enregistré des pertes allant jusqu'à 245 millions de dollars en raison de la cyberfraude[17], somme élevée pour des pays dont les systèmes bancaires ne sont pas très développés. Plusieurs banques commerciales de Zambie[18] ont été dépouillées de plus de 4 millions de dollars au premier semestre de 2013 à la suite de l'association de cybercriminels zambiens et étrangers chevronnés.

## 3. Les défis de la cybersécurité en Afrique

L'Afrique est face à plusieurs défis liés à Internet: risque pour la sécurité, viol de la propriété intellectuelle et protection des données personnelles. Les cybercriminels ciblent des particuliers à l'intérieur et à l'extérieur de leurs frontières nationales et les gouvernements africains n'ont pas les moyens techniques et financiers de cibler et de suivre les échanges électroniques jugés sensibles pour la sécurité nationale.

Ces défis sont les suivants:

- Faiblesse du niveau des dispositions de sécurité nécessaires pour prévenir et maîtriser les risques technologiques et informationnels.
- Manque de savoir-faire technique en matière de cybersécurité et incapacité

14 Symantec Corporation, *2012 Norton Cybercrime Report*, septembre 2012.

15 International Data Group Connect, "Africa 2013: Cyber-crime, hacking and malware", White Paper. Disponible à l'adresse www.idgconnect.com/view_abstract/11401/africa-2013-cyber-crime-hacking-malware.

16 Business Software Alliance, "Shadow market: 2011 BSA global software piracy study", neuvième édition, mai 2012. Disponible à l'adresse http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

17 Henry Quarshie et Alexander Martin-Odoom, "Fighting Cybercrime in Africa", *Computer Science and Engineering*, vol. 2, No. 6 (2012), pp. 98-100.

18 Michael Chawe, «Cyber crime costs Zambian banks $4m», Africa Review, 14 juin 2013, Disponible à l'adresse www.africareview.com/News/Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html.

de surveiller et de défendre les réseaux nationaux, rendant les pays africains vulnérables au cyberespionnage ainsi qu'au cyberterrorisme.

- Incapacité à mettre en place les cadres juridiques nécessaires pour lutter contre la cybercriminalité. Une enquête menée par la CEA[19] auprès de 21 pays a permis de constater que si de nombreux pays ont proposé des législations, peu de systèmes de sécurité permettant de lutter contre la cybercriminalité ont été installés, tant dans le secteur privé que dans le secteur public.
- Les enjeux de la cybersécurité ont une portée plus large que ceux de la sécurité nationale. Pourtant, peu d'initiatives majeures ont été mises en œuvre en Afrique dans le domaine de la cybersécurité. Alors que les TIC sont saluées comme la panacée aux nombreux problèmes de l'Afrique, la cybersécurité est une question cruciale qui doit être abordée plus en profondeur.
- Il est nécessaire de mettre en place une société de l'information qui respecte les valeurs, les droits et les libertés et qui garantit l'égalité d'accès à l'information tout en encourageant la création de connaissances authentiques et en renforçant la confiance dans l'utilisation des TIC en Afrique.
- D'une manière générale, les parties prenantes, comme les organes de réglementation des TIC, les organismes chargés de l'application des lois, la justice, les professionnels de la technologie de l'information et les utilisateurs sont peu conscients des problèmes de sécurité liés aux TIC.

19 Bénin, Burundi, Congo, Côte d'Ivoire, Égypte, Éthiopie, Gambie, Ghana, Guinée-Bissau, Kenya, Madagascar, Mali, Mozambique, Niger, Nigéria, Ouganda, République démocratique du Congo, Sénégal, Soudan, Togo et Zambie.

## 4. Recommandations stratégiques

Il est difficile de mesurer l'ampleur des défis posés par les lacunes en matière de cybersécurité. La cybercriminalité est de nature transnationale. Par conséquent, la lutte contre la cybercriminalité exige des stratégies coordonnées et ciblées. La multiplicité des questions exige de tenir compte de leurs multiples aspects, à savoir, scientifiques, technologiques, économiques et financiers, politiques et socioculturels. L'interaction entre ces aspects accroit la complexité de la cybersécurité, qui se manifeste à plusieurs niveaux.

### *4.1 Mécanismes stratégiques, juridiques et réglementaires*

Le continent étant de plus en plus tributaire des TIC, les particuliers, les organisations et les pays sont très vulnérables aux attaques des systèmes et réseaux d'information (piratage, cyberterrorisme et cybercriminalité). Peu de particuliers et d'organisations sont équipés pour faire face à de telles attaques. À cet égard, le rôle des pouvoirs publics dans le traitement de cet important phénomène ne saurait être surestimé. Le succès d'une éventuelle initiative sur la cybersécurité dépend de la participation et du soutien inconditionnels des dirigeants politiques au plus haut niveau. Le rôle des gouvernements dans la mise en place d'un cadre politique, juridique et réglementaire est d'une importance primordiale, à savoir:

#### *4.1.1 Cadre juridique*

L'absence de loi sur la cybersécurité est préjudiciable aux opérations commerciales. Il est donc essentiel que toutes les parties prenantes mettent en place des lois et règlements efficaces sur le pollupostage et la cybercriminalité afin de rétablir la confiance dans l'utilisation d'Internet, notamment pour les transactions en ligne. Ces mesures devraient être accompagnées d'un renforcement des capacités des parties prenantes politiques concernées et de la création d'un cadre local de lutte contre la cybercriminalité.

#### *4.1.2 Harmonisation des cadres stratégiques et juridiques*

La question de l'harmonisation est distincte de la question ci-dessus tout en y étant très étroitement liée. Bien que les États membres soient à des stades différents de la lutte contre la cybersécurité et de la mise en place d'instruments stratégiques et de cadres législatifs, il est essentiel d'harmoniser les cadres stratégiques et juridiques compte tenu de l'ampleur mondiale de la cybercriminalité.

La cybersécurité est un bien mondial qui appelle des mesures sur le plan mondial et régional. Il est nécessaire de fixer des normes et procédures minimales pour que le continent puisse fonctionner comme une entité homogène et pour que les mesures qu'il prend soient efficaces. À cet égard, la Commission de l'Union africaine (CUA) et la CEA ont chapeauté les efforts de développement de la Convention de l'Union africaine sur la cybersécurité, qui a fait l'objet d'une série d'examens par les communautés économiques régionales puis a été entérinée par la Conférence ordinaire de l'Union africaine en charge des technologies de l'information et des communications en septembre 2012 à Khartoum, et enfin adoptée par le Sommet des chefs d'État et de gouvernement de l'Union africaine de juin 2014 à Malabo. On s'attend, par conséquent, à ce que les pays dotés d'une législation sur la cybersécurité la transposent dans le cadre de la Convention et que ceux qui n'en n'ont pas encore soient aidés à s'en doter.

#### *4.1.3 Coordination et coopération*

La cybersécurité ne connait pas de frontières et, compte tenu de sa dimension mondiale, il est difficile de prendre des mesures au seul niveau national. La lutte contre les atteintes à la cybersécurité nécessite une coopération à tous les niveaux, entre les pays et les organisations internationales, et entre les secteurs public et privé. Par conséquent, un cadre global de coopération et de sensibilisation internationales doit être mis en place. Pour ce faire, la coordination et la coopération dans des domaines comme la fraude, le piratage, la distribution d'images pédopornographiques et la violation du droit d'auteur par des moyens informatiques, ainsi que l'uniformisation des procédures sont essentielles.

### *4.2 Considérations technologiques*

#### *4.2.1 Mise en place d'infrastructures et de services*

- Il doit exister des infrastructures de réseaux nationaux dédiés reliant le gouvernement, l'industrie et la communauté de la recherche afin d'encourager le partage ouvert des connaissances, la mise en place d'un système ouvert de données pour les chercheurs, l'innovation, les synergies entre les utilisateurs finaux et les chercheurs et le développement des technologies de l'information.
- Il est également nécessaire de mettre en place un écosystème national de préparation aux situations d'urgence et une équipe d'intervention informatique afin d'encourager les synergies nationales sur la cybersécurité, le partage des connaissances et la collecte de renseignements sur les mesures de lutte contre la cybercriminalité préjudiciable aux États ainsi qu'aux particuliers.
- Un centre d'appel dédié devrait être mis en place afin que les victimes de la cybercriminalité sachent qu'il existe un endroit vers lequel elles peuvent se tourner pour dénoncer ces délits et recevoir de l'aide. Dans le cadre de la stratégie globale de cybersécurité, le centre d'appel devrait être doté d'un personnel suffisamment formé et compétent et disposer d'un site Web et d'un numéro d'appel gratuit pour permettre aux victimes de signaler un délit avec un minimum de désagréments.
- La diffusion des bonnes pratiques des fournisseurs de services Internet et des efforts qu'ils déploient pour réduire la cybercriminalité, et le renforcement des capacités des fournisseurs de services en commerce électronique et transactions en ligne devraient être encouragés.

*4.2.2 Investissement dans la recherche*

Les connaissances et l'information sont un moyen direct d'autonomisation des pays et de leurs citoyens. Actuellement, l'Afrique souffre d'un manque général de connaissances et d'information sur les questions liées à la cybersécurité. Ce manque doit être comblé. Pour ce faire, des ressources suffisantes doivent être investies dans la recherche sur la cybersécurité en Afrique, qui fait actuellement défaut. Dans les cas où des recherches ont été entreprises, les résultats ne sont pas facilement disponibles ou accessibles. Par conséquent, des banques de données doivent être créées de façon que les chercheurs puissent y déposer les résultats de leurs travaux, y compris les outils et les techniques employés pour trouver et recueillir des informations sur la cybercriminalité. Plusieurs pays ont voté des lois sur le dépôt des données. Celles-ci s'étant révélées très utiles, les pays qui ne sont pas encore dotés de telles lois devraient le faire en appliquant les bonnes pratiques des pays qui les ont précédé dans ce domaine.

### *4.3 Les dimensions sociales*

*4.3.1 Éducation*

L'accroissement des compétences nécessaires ne progresse pas au même rythme que la croissance exponentielle de l'utilisation du cyberespace en Afrique. Des initiatives d'éducation générale sur la sûreté et la sécurité Internet doivent donc être lancées pour résoudre les questions liées à la protection de l'enfance et à la sécurité dans la société en général. En outre, la facilitation d'un accès sécurisé aux TIC est d'une importance primordiale pour les utilisateurs.

*4.3.2 Participation de l'ensemble des parties prenantes clés*

Il est important de comprendre qu'aucune personne ou institution n'a la capacité nécessaire pour assurer, à elle seule, la cybersécurité. La cybersécurité ne se limite pas à un phénomène; c'est un processus. Elle ne se limite pas à l'adoption d'une loi ou à l'intervention exclusive des juristes. Les parlementaires, les juristes, les magistrats, les services de renseignement, les militaires, la société civile, les médias, les jeunes et les membres du public sont les principales parties prenantes qui doivent toutes contribuer, le plus rapidement possible, aux efforts en matière de cybersécurité. Il est important de rallier toutes les parties prenantes pour qu'elles comprennent les problèmes et les processus en jeu.

## Références


Atta-Asamoah, Andrews. (juillet 2010). Understanding the West African cyber-crime process. African Security Review Vol. 18 No.4 pages 105-114. Institute for Security Studies. http://www.tandfonline.com/doi/s/10.1080/10246029.2009.9627562?journalCode=rasr20#.Uu9NOPtdx8E.

Kaiko Namusa,Cyber crime costs banks $4m. Times of Zambia. http://www.times.co.zm/?p=18423 http://www.africareview.com/News/Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html

Office des Nations Unies contre la drogue et le crime (février 2013) Étude approfondie sur la cybercriminalité.
http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_ STUDY_210213.pdf

***Cette note d'orientation a été élaborée par M. Mactar Seck, avec la collaboration de Mme Tsega Belai sous la supervision de M. Kasirim Nwuke, Chef de la Section des nouvelles technologies et de l'innovation/Division des initiatives spéciales.***


**Contact**

Pour obtenir davantage de renseignements sur le programme de la CEA en matière de technologie et d'innovation, veuillez contacter M. Kasirim Nwuke, Chef de la Section des nouvelles technologies et de l'innovation/Division des initiatives spéciales, tél.: +251 (0) 11 544-3375, télécopie: +251 (0) 11 551-0512, courriel: Knwuke@uneca.org.



**Commandes**

Pour commander des exemplaires de *Relever les défis de la cybersécurité en Afrique*, note d'orientation n° NTIS/002/2014 de la Commission économique pour l'Afrique:

**Veuillez contacter:**

Publications
Commission économique pour l'Afrique
P.O. Box 3001, Addis-Abeba, Éthiopie
Tél.: +251 11 544-9900
Télécopie: +251 11 551-4416
Courriel: ecainfo@uneca.org

Site Web: www.uneca.org