

DECRYPTAGE DES MENACES SECURITAIRES A L'ERE DE LA CYBERCRIMINALITE EN AFRIQUE POST GUERRE-FROIDE

par

Jean-Hervé MBELU BIOSHA

Professeur Associé, Faculté des Sciences Sociales,
Université de Kinshasa

Résumé

Le monde fait face actuellement à un éventail croissant de cybermenaces et de défis auxquels les stratégies de cybersécurité devraient être adoptées à toutes les échelles possibles. Ainsi, cette réflexion s'efforce, d'une part, à faire un portrait analytique de la cybercriminalité en Afrique post guerre et, d'autre part, à s'interroger sur la politique africaine en la matière, tout en relevant sa portée, sa mise en œuvre et des leçons qui en découleraient.

Mots-clés : *cybermenace, cybercriminalité, cyberattaque, menace sécuritaire, Afrique post guerre-froide*

Abstract

The entire world is currently facing a growing range of cyber threats and challenges, requiring cybersecurity strategies to be adopted at all possible levels. This paper therefore seeks, on the one hand, to provide an analytical portrait of cybercrime in post-Cold War Africa and, on the other, to examine African policy in this area, while highlighting its scope, implementation, and lessons learned.

Keywords : *cyberthreat, cybercrime, cyberattack, security threat, post-Cold War Africa*

INTRODUCTION

L'essor rapide des nouvelles technologies crée des opportunités dans la région africaine. C'est présentement en Afrique que les réseaux Internet et de téléphone connaissent le développement le plus rapide au monde et que l'utilisation des services bancaires mobiles est largement répandue¹. Néanmoins, cette migration éclaire vers le numérique expose la région à des cyberattaques.

De plus en plus d'entreprises et d'institutions publiques sont devenues la cible des hackers qui piratent leurs serveurs et réclament ensuite une rançon. Les entreprises africaines se trouvent de plus en plus sous la menace de cyberattaques, évidemment. Ces dernières sont très souvent transfrontalières. C'est en ces termes que Assih Palakiyem² confirme l'exposition des entreprises du continent aux attaques informatiques. Aucun secteur n'est épargné. Selon lui, à partir du moment où on est connecté à l'Internet, on est potentiellement victime d'une cyberattaque.

En conséquence, de nombreux gouvernements africains ont adopté, avec empressement, de nouvelles lois sur la cybercriminalité afin de suivre le rythme et de continuer à se protéger contre les crimes commis en ligne. De nos jours, au moins une quarantaine d'États africains disposent d'une législation de base en matière de cybercriminalité, soit entièrement soit partiellement, bien qu'il manque à beaucoup d'entre eux des règlements d'application. L'Union Africaine, pour sa part, n'est pas en reste. La 23^{ème} Assemblée des chefs d'Etat et des gouvernements de l'UA, tenue à Malabo les 26-27 Juin 2014, a adopté la « Convention sur la cyber sécurité et la protection des données à caractère personnel ». Qu'à cela ne tienne, la cybercriminalité, sous ses différentes formes, continue son bonhomme de chemin avec des conséquences néfastes que l'on ne cessera de décrier.

Sous l'angle méthodologique, la démarche suivie lors du recueil des données a reposé essentiellement sur la technique d'entretien libre avec notamment les gestionnaires de serveurs des institutions telles que gouvernement, banques, services de renseignement sans oublier arnaqueurs incriminés. Aux renseignements obtenus de cette technique de recherche, se sont ajoutés ceux puisés de la documentation relevant de diverses sources écrites. Les données ainsi rassemblées ont été analysées à la lumière des postulats dialectiques qui ont permis de mettre à nu les contradictions qui alimentent la cybercriminalité et leurs conséquences.

Enfin, cette réflexion s'efforce, d'une part, à faire un portrait analytique de la cybercriminalité en Afrique post guerre et, d'autre part, à s'interroger sur la politique africaine en la matière, tout en relevant sa portée, sa mise en œuvre et des leçons qui en découlent.

¹ <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique>.

² <https://www.dw.com/fr/afrique-cybercriminalit%C3%A9/a-61251435>.

I. APPREHENSION DES MENACES SECURITAIRES EN AFRIQUE POST GUERRE-FROIDE

Depuis la fin de la guerre froide, la littérature en relations internationales et en études stratégiques s'attarde tout particulièrement à l'émergence de nouvelles menaces à la sécurité qui se distinguent par rapport à la menace militaire classique. Ce sont désormais les guerres intraétatiques ainsi que les menaces de type non militaire qui sont devenues un objet central d'analyse. David J. Francis³, avec son livre *Uniting Africa*, s'inscrit au sein même de cette littérature. Il soutient que la gestion de ces menaces émergentes de l'ère post-guerre froide doit s'effectuer par le mécanisme de l'intégration régionale et du régionalisme.

De notre point de vue, les menaces sécuritaires tant à travers le monde qu'en Afrique, ont pris d'autres dimensions par rapport à celles qui ont prévalu à l'époque de la guerre froide. Ces menaces, issues jadis de diverses causes, ne proviennent pas toutes nécessairement de l'extérieur du continent. Elles émanent également de l'intérieur, notamment : la mauvaise gouvernance, la pauvreté, la corruption, le chômage, les maladies, les questions environnementales, les médias, le terrorisme, la cybercriminalité, le tribalisme, la montée de l'extrémisme et la présence des gisements immenses des minerais.

Pour dire davantage, Cyril Robinet⁴ note avec instance que conflits, migrations incontrôlées, djihadisme, réseaux criminels, États défaillants en Afrique, les nouveaux risques sécuritaires sont désormais liés avant tout, à des questions de (mauvaise) gouvernance et de (mal) développement.

Pour André Dumoulin⁵, les bouleversements géopolitiques et géostratégiques de ces dernières années ont fait disparaître les traditionnels repères, simples et relativement stables qui caractérisaient les relations internationales durant la guerre froide. Avec la fin des blocs, le monde est à la fois globalement plus sûr mais politiquement plus incertain. L'Europe est moins menacée aujourd'hui qu'hier même si certaines crises périphériques peuvent encore, en partie, attenter à sa stabilité. Néanmoins, pour chacun des argumentaires des nouvelles menaces (reconstitution d'une armée russe menaçante, une Chine conquérante, les différentes proliférations, la poussée de l'islam intégriste, les nationalismes belligères et les grands défis globaux de notre temps), il y a lieu de déterminer une échelle de grandeur et de « plausibilité » de celles-ci, entreprendre une pondération du niveau des menaces et préciser leur implication véritable sur la sécurité du continent européen.

En réalité, dans bien des hypothèses, le traitement militaire de ces menaces n'est ni souhaitable ni crédible, la sécurité ne pouvant plus reposer exclusivement sur des structures interventionnistes militaires. Les remèdes à ces nouvelles menaces passent plutôt par des interventions d'ordre politique, économique, social, diplomatique, juridique et finalement d'interposition.

De son côté, Pierre du Bois⁶ révèle que les experts de l'Union européenne en distinguent cinq types : le terrorisme, religieux en particulier ; la prolifération des armes de destruction de masse, qui comprennent les armes atomiques, les armes biologiques et les armes chimiques ; les conflits régionaux ; la déliquescence de l'État ; la criminalité organisée. Comme telle, la liste est incomplète et inappropriée à une vision globale des insécurités réelles. D'autres experts mentionnent la violence civile, avec des manifestations de masse plus ou moins dramatiques, les migrations clandestines, les catastrophes naturelles et les atteintes à l'environnement, voire la pauvreté et les épidémies. En tout état de cause, la réflexion suppose une approche élargie du concept de menace. Elle implique aussi un examen de la perception de la menace. L'époque actuelle met plutôt l'accent sur une notion assez large de sécurité, qui a débouché sur l'expression de « sécurité humaine » employée par les Nations Unies

Cependant, dans l'ère post guerre-froide, le monde étant devenu un village planétaire où les frontières physiques sont quasi-inexistantes soutenues par les mouvements des populations d'un Etat à un autre et le développement des Nouvelles Technologies de l'Information et de la Communication, dans ce nouveau monde, la conception des menaces sécuritaires a évolué. Ces menaces sont dorénavant multiples et plurielles, obligent même les gouvernants à revoir leurs politiques par rapport à cette nouvelle réalité. Malheureusement, les dirigeants politiques, avides de pouvoir, installés durant des

³ J-D. FRANCIS, *Uniting Africa. Building Regional Peace and Security Systems*, Aldershot, Ashgate, 2007, p. 278.

⁴ <https://www.vie-publique.fr/parole-dexpert/271196-afrique-le-defi-de-la-securite>, consulté le 16 janvier 2023 à 08 heures 27 minutes.

⁵ Lire avec intérêt A. DUMOULIN, *Risques et menaces dans un monde en mutation*, Paris, 1992.

⁶ P. du BOIS, « Anciennes et nouvelles menaces : les enjeux de la sécurité en Europe », in *Dans Relations internationales* 2006/1 (n° 125), pages 5 à 16

années au sommet de l'État, assurent leur longévité et leur survie politiques grâce à la force et à l'insécurité.

Sous l'effet de la globalisation de l'information et des migrations internationales, le monde est devenu « un village planétaire ». Du point de vue des relations internationales, le libéralisme, l'idéalisme et le constructivisme, les sociétés, les Etats, de plus en plus interdépendants, élaborent de nouvelles solidarités. La perception holiste des problèmes de sécurité s'impose à tous sur des thématiques universelles : environnement, eau, écologie et biodiversité, grippe aviaire, épidémie, pandémie, VIH-Sida, cybercriminalité, terrorisme international, les drogues, les « coupeurs de route », etc. A cet effet, la notion de souveraineté étatique devient plus atténuée.

Notre ère multidimensionnelle, « multi-centrée », est aussi celle d'interpénétration de structures de contrôle social, d'allocation de surveillance sanitaire et de pauvreté. Le droit international humanitaire, par le droit d'ingérence humanitaire et les conventions sur les crimes contre l'humanité, traverse plus facilement les frontières des Etats. La grille de lecture des menaces, des vulnérabilités et risques souligne la forte interaction entre le local, le national et l'international. En clair, un degré différent, en phase de transition démocratique et souscrivent tous aux programmes de gouvernance démocratique. Pour préserver leur sécurité respective, des accords de défense et d'assistance/coopération militaire, de soutien logistique, établis avant 1960, les lient avec les anciennes métropoles.

Ces phénomènes apparaissent toujours comme la conséquence directe de l'échec d'un modèle de construction d'un Etat postcolonial caractérisé par Etat ne saurait garantir sa propre sécurité qu'en menaçant celle des autres : c'est le dilemme de la sécurité ! Face à la fragilité des initiatives nationales, la sécurité collective et coopérative formule de meilleures perspectives de paix, de sécurité, caution d'un développement durable.

D'ailleurs, dans notre thèse de doctorat, nous avons souligné que « *le contexte régional et mondial représente aujourd'hui de nouveaux enjeux sécuritaires auxquels la communauté internationale tout comme chaque pays, pris à part, doit faire face. C'est un virage qui débouche les yeux sur les visages modernes de l'insécurité et de la violence. Il est évident que les menaces plus classiques mais tout aussi dangereuses persistent. Mais en devenant une menace directe et ouverte pour l'individu, l'insécurité prend de nouvelles dimensions. Elle est plus proche, plus quotidienne et donc plus dangereuse* »⁷.

Traditionnellement, l'idée de sécurité et de défense est intimement liée à celle de l'Etat. Mais cette sécurité nationale est maintenant tournée vers la sécurité humaine, c'est-à-dire vers l'individu et la collectivité. C'est une nouvelle approche devenue incontournable dans la mesure où les civils sont, malheureusement, devenus la proie des conflits et les premières victimes.

II. ERE DE LA CYBERCRIMINALITE EN AFRIQUE POST GUERRE-FROIDE : GENESE, TYPOLOGIE ET PROPORTION

L'essor rapide des nouvelles technologies crée des opportunités dans la région africaine. En effet, c'est actuellement en Afrique que les réseaux Internet et de téléphone connaissent le développement le plus rapide au monde et que l'utilisation des services bancaires mobiles est largement répandue. Néanmoins, cette migration éclair vers le numérique expose la région aux cyberattaques. Il s'agit bien de la cybercriminalité⁸. L'Interpol⁹ opine, cependant, que les criminels tirent parti de l'utilisation accrue des Smartphones en volant des données à caractère personnel et montant des mécanismes frauduleux.

En Afrique, le rapport de l'Interpol¹⁰ renseigne que les principales cybermenaces sont les escroqueries aux faux ordres de virement (FOVI), le hameçonnage, les rançongiciels, les chevaux de Troie bancaires et les voleurs d'informations, les escroqueries en ligne, la cyberextorsion et les logiciels criminels.

⁷ J-H. MBELU BIOSHA, *op. cit.*, p. 233.

⁸ Il n'existe pas de définition précise et universelle du terme « cybercriminalité ». En termes généraux, il s'agit d'un délit qui est commis en utilisant un réseau informatique ou l'Internet. Cela peut couvrir un large éventail d'activités, y compris les activités terroristes et l'espionnage menés à l'aide d'Internet et le piratage illégal de systèmes informatiques, les infractions liées au contenu, le vol et la manipulation de données, et le cyberharcèlement.

⁹ Lire in <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique-AFJOC>, consulté le 15 janvier 2023 à 22 heures 27 minutes.

¹⁰ INTERPOL, *Rapport d'évaluation des cybermenaces en Afrique. Présentation des principales cybermenaces par le desk africain pour les opérations de lutte contre la cybercriminalité*, Mars 2023, pp. 11-13.

En effet, les *escroqueries aux faux ordres de virement* consistent à obtenir un accès non autorisé au compte de messagerie d'une organisation et à l'utiliser pour envoyer des messages frauduleux à ses partenaires commerciaux dans un but lucratif.

L'hameçonnage consiste à voler des informations sensibles telles que les noms d'utilisateur, les mots de passe et les coordonnées bancaires appartenant à des victimes non averties.

Les *rançongiciels* sont une forme malveillante de logiciels qui bloquent l'accès des utilisateurs à leurs propres données, systèmes et appareils en cryptant leurs fichiers. Une fois le cryptage terminé, les victimes reçoivent un message les informant qu'elles doivent s'acquitter d'une certaine somme pour que leurs fichiers soient décryptés et qu'elles puissent à nouveau y accéder.

Les *chevaux de Troie bancaires et les voleurs d'informations* sont des logiciels malveillants destinés à voler des informations sensibles telles que les noms d'utilisateur, les mots de passe et les données financières appartenant à des victimes non averties. Ces chevaux de Troie peuvent être installés via des courriels d'hameçonnage, des sites Internet malveillants, des téléchargements furtifs ou d'autres moyens. Une fois le cheval de Troie installé sur l'ordinateur de la victime, il tente d'accéder à ses comptes bancaires en ligne en enregistrant la frappe ou en volant les identifiants de connexion.

Les *escroqueries en ligne* sont la forme la plus courante et la plus dangereuse d'escroquerie, dont la dimension est internationale. Les escroqueries en ligne désignent tout type d'infraction frauduleuse commise via un ordinateur ou à l'aide de données informatiques

La *cyberextorsion* consiste, pour un criminel, à utiliser des techniques numériques pour menacer des victimes ou leur extorquer de l'argent et/ou d'autres actifs. En règle générale, le cybercriminel menace de révéler des informations personnelles gênantes, de supprimer des données importantes, de saboter des systèmes et réseaux, ou encore de lancer une attaque par déni de service distribué

Les *logiciels criminels* en tant que service, ou CaaS, désignent un programme ou un ensemble de programmes informatiques destinés à faciliter les activités illégales en ligne. Les logiciels espions, les kits d'hameçonnage, les pirates de navigateur, les enregistreurs de frappe et bien d'autres outils malveillants sont mis à la disposition des cybercriminels sous forme de CaaS.

Par ailleurs, Mediadefence¹¹ retient la violation de la confidentialité des données, la criminalisation de la parole en ligne, le cyberharcèlement, le harcèlement en ligne et la cyberintimidation comme les principaux types de la cybercriminalité.

Cependant, étant donné que la Convention de Malabo n'a pas encore été testée dans la pratique, une lecture de la Convention de Budapest sur la cybercriminalité, le premier traité international qui vise à lutter contre les crimes sur Internet et les crimes informatiques, est instructive¹². Elle est de plus en plus utilisée en Afrique et a servi de ligne directrice ou de source à plus de 80% des États du monde entier pour élaborer des lois nationales sur la cybercriminalité¹³. Elle est également ouverte à tout État désireux d'appliquer ses dispositions et peut être ratifiée par les pays africains¹⁴.

La Convention de Budapest¹⁵ définit les types de cybercriminalité suivants : l'accès illégal à un système informatique, l'interception illégale, l'interférence dans les données, l'interférence du système, l'utilisation abusive des appareils, la falsification informatique, la fraude informatique, la pornographie infantine et les infractions liées aux violations du droit d'auteur et des droits voisins. Bien que ces définitions datent de 2001, une grande partie de ce qui constitue aujourd'hui la cybercriminalité est toujours couverte par ces catégories et dispositions.

En ce qui concerne l'Afrique, l'absence de normes en matière de cybersécurité dans la quasi-totalité des États africains expose les services en ligne à des risques majeurs. Les cyberattaques ciblant les infrastructures critiques comme les banques et les organismes publics, sont exposés à de graves conséquences : risques de sécurité, pertes financières considérables et perturbation des activités.

Ainsi, la cybercriminalité s'est amplifiée avec le développement de l'Internet, pour atteindre des proportions inquiétantes. Tel est le constat de certains des participants de la première conférence

¹¹ Mediadefence, *Op. cit.*, p. 9.

¹² Conseil de l'Europe, *L'état de la législation sur la cybercriminalité en Afrique - un aperçu*, 2015, p. 2.

¹³ Conseil de l'Europe, *The global state of cybercrime legislation 2013 – 2020 : A cursory overview*, 2020, p. 5.

¹⁴ Conseil de l'Europe, *État des signatures et ratifications du Traité 185*, 2020.

¹⁵ Conseil de l'Europe ci-dessus, au point n° 48, p. 8.

régionale sur la cybersécurité, dans la capitale politique de la République de Côte d'Ivoire. Malgré son faible nombre d'internautes (24 millions, soit 2,6 % du total mondial), l'Afrique est devenue un terrain d'action important pour les cybercriminels¹⁶. Selon Sylvanus Kla, directeur général de l'Agence de télécommunication de Côte d'Ivoire, la délinquance informatique est en nette augmentation sur le continent.

III. AUTOUR DE LA POLITIQUE AFRICAINE CONTRE LA CYBERCRIMINALITE : PORTEE, MISE EN ŒUVRE ET LEÇONS A TIRER

Pour réagir aux difficultés liées à la législation posées par les activités criminelles, commises sur les réseaux de TIC, d'une manière compatible au niveau régional et continental et aussi en réponse à la nécessité d'harmoniser les législations dans le domaine de la cyber sécurité et la protection des données à caractère personnel dans les Etats membres de l'Union Africaine, la 23^{ème} Assemblée des chefs d'Etat et des gouvernements de l'UA, tenue à Malabo les 26-27 juin 2014, a adopté la « Convention sur la cyber sécurité et la protection des données à caractère personnel » de l'Union Africaine qui est aussi dénommée la « Convention de Malabo ».

Dans son contenu, cette politique africaine¹⁷ prévoit des mesures de cybersécurité à prendre au niveau national. Et, comme cadre de la cybersécurité nationale¹⁸, elle a prévu la mise en œuvre d'une politique nationale à travers laquelle chaque État Partie, devrait s'engager en collaboration avec les parties prenantes, à se doter d'une politique nationale de cyber sécurité qui reconnaisse l'importance de l'infrastructure essentielle de l'information (IEI) pour la nation, qui identifie les risques auxquels elle est confrontée en utilisant une approche tous risques et qui, définit, dans les grandes lignes, la façon dont les objectifs seront mis en œuvre. Toujours dans le registre du cadre de la cybersécurité nationale, la convention a prévu une stratégie nationale à partir de laquelle les États Parties devraient s'engager à adopter les stratégies qu'ils jugent appropriées et suffisantes pour mettre en œuvre la politique nationale de cyber sécurité, spécifiquement dans le domaine de la réforme législative et du développement, de la sensibilisation et du développement des capacités, du partenariat public- privé et de la coopération internationale, pour ne citer que ceux-ci. Les stratégies devront établir des structures organisationnelles et se fixer des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cyber sécurité, tout en posant les bases d'une gestion effective des incidents et de la coopération internationale.

Par conséquent, la cybersécurité et la cybercriminalité ne peuvent pas être traitées comme n'importe quel autre sujet réglementaire. Pour les pays africains, il est nécessaire de considérer la cybercriminalité comme un problème important au niveau national et régional qui affecte leurs souverainetés et leurs sécurités nationales, ainsi que la protection des sociétés et des infrastructures critiques.

Bien que ces efforts régionaux visant à élaborer et à mettre en œuvre une cyber-stratégie soient dignes d'intérêt, ils ne seront efficaces que s'ils catalysent une coordination et une coopération à grande échelle au niveau national pour lutter contre la cybercriminalité organisée transfrontalière, l'extrémisme violent et les activités malveillantes parrainées par des États dans le cyberspace. Les efforts précédents visant l'amélioration de la cybercoopération transfrontalière en Afrique, notamment la Convention sur la cybersécurité et la protection des données personnelles (Convention de Malabo) parrainée par l'UA, ont échoué précisément, en raison du manque d'un soutien adéquat au niveau national. Pour ce faire, il faut, comme point de départ, mettre en place des stratégies et des politiques cohérentes en matière de cybersécurité au niveau national.

Malheureusement, les progrès réalisés dans l'élaboration et la mise en œuvre d'une stratégie de cybersécurité au niveau national en Afrique sont limités. De ce fait, Abdul-Hakeem Ajjola et Nate Allen¹⁹ soutiennent que selon les données les plus récentes compilées par l'Union Internationale des Télécommunications des Nations Unies, environ un tiers (17) des 54 pays d'Afrique ont élaboré une

¹⁶ J-J. BOGUI, « La cybercriminalité, menace pour le développement. Les escroqueries Internet en Côte d'Ivoire », in *Dans Afrique contemporaine*, 2010/2, n° 234, pp. 155-170.

¹⁷ Pour plus d'informations, lire Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel.

¹⁸ Article 24 de la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel.

¹⁹ A-H. AJJOLA et D.F. ALLEN, « Leçons d'Afrique en matière de cyber-stratégie », in <https://africacenter.org/fr/spotlight/lecons-dafrique-en-matiere-de-cyber-strategie>, consulté le 14 janvier 2024 à 17 heures 17 minutes.

stratégie nationale de cybersécurité, ce qui représente moins de la moitié de la moyenne mondiale. Les gouvernements sont l'acteur le plus important en matière de gestion des cybermenaces²⁰. En l'absence de stratégies nationales, les gouvernements se trouvent souvent dans l'incapacité de définir la portée et l'ampleur des menaces auxquelles ils sont confrontés, de fixer des priorités, de mobiliser des ressources ou de coordonner efficacement les réponses au sein du gouvernement, avec le secteur privé et les acteurs communautaires.

Moins de la moitié des pays dotés d'une stratégie nationale de cybersécurité disposent d'une évaluation des menaces (qui permet de justifier l'existence de la stratégie et d'adapter la réponse à la menace) ou d'une affectation des ressources (qui est nécessaire pour assurer la mise en œuvre d'une stratégie).

Stratégies nationales africaines en matière de cybersécurité						
Pays	Évaluation des menaces	Plan d'action	Calendrier	Attribution des responsabilités	Affectation des ressources	Dernière mise à jour
Bénin	✓	✓		✓		2020
Burkina Faso		✓				2019
Égypte	✓	✓	✓			2018
Eswatini	✓	✓	✓	✓	✓	2020
Gambie		✓		✓		2016
Ghana		✓	✓	✓		2020
Kenya	✓	✓	✓	✓	✓	2014
Malawi		✓	✓	✓	✓	2017
Maurice		✓	✓	✓		2014
Maroc		✓	✓	✓	✓	2013
Nigeria	✓	✓	✓	✓		2021
Rwanda		✓	✓	✓	✓	2015
Sénégal	✓	✓	✓	✓	✓	2017
Sierra Leone	✓	✓	✓		✓	2017
Afrique du Sud		✓		✓		2012
Tanzanie		✓		✓		2016
Ouganda		✓				2014
TOTAL	7	17	11	13	7	

Source : Abdul-Hakeem Ajijola et Nate D.F. Allen, *art. cit.*

Malheureusement, suivant le tableau ci-haut, les stratégies nationales de cybersécurité de trois pays africains seulement (l'Eswatini, le Kenya et le Sénégal) répondent aux critères minimaux essentiels. Il s'agit notamment d'une évaluation des menaces qui identifie la portée et l'ampleur des cybermenaces d'un pays, un plan d'action qui contient des objectifs et des activités concrets destinés à faire face aux menaces, un calendrier, une répartition des responsabilités entre les principales parties prenantes et des dispositions claires en matière d'affectation des ressources.

Dans le même registre, il est important de relever l'étude menée par Interpol et Afripol²¹ contre la cybercriminalité. Les services chargés de l'application de la loi de 27 pays membres d'INTERPOL ont uni leurs forces dans le cadre de l'opération Cyber Surge Afrique pour lutter contre la cybercriminalité à travers le continent. Coordinée depuis un centre de commandement INTERPOL à Kigali, au Rwanda, l'opération a eu pour but de neutraliser les catalyseurs de la cybercriminalité. Les principaux résultats de l'opération sont :

- onze individus ont été arrêtés, dont un suspect en lien avec des abus pédosexuels et dix autres impliqués dans des escroqueries et des actes frauduleux représentant 800 000 USD, ayant fait des victimes dans le monde entier ;

²⁰ N. ALLEN et C. LENA KELLY, « Un déluge de répression numérique menace la sécurité africaine », in *Éclairage*, Centre d'études stratégiques de l'Afrique, 13 janvier 2022.

²¹ <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2022/Une-operation-a-travers-le-continent-africain-permet-d-identifier-des-cybercriminels-et-les-infrastructures-virtuelles-a-risque>.

- les autorités érythréennes ont démantelé un cryptomarché qui proposait des outils de piratage et des composants relatifs à la cybercriminalité en tant que service ;
- plusieurs affaires d'escroquerie aux cybermonnaies ont été résolues au Cameroun, dont une dans laquelle la victime avait subi un préjudice financier estimé à plus de 8 millions CFA ;
- la Tanzanie a recouvré plus de 150 000 USD dérobés à des victimes dans le cadre d'affaires d'atteinte à la protection des données et au droit d'auteur.

Des mesures ont été prises contre plus de 200 000 éléments d'infrastructure virtuelle malveillante qui facilitaient la cybercriminalité à travers l'Afrique. L'infrastructure malveillante, qui a été démantelée et nettoyée, servait de réseau de machines zombies et menait des activités d'hameçonnage, d'envoi de courriers indésirables et de cyberextorsion (ex. escroqueries aux sentiments, escroqueries bancaires et vol de données) à grande échelle. Ce fut également l'occasion pour les pays participants de renforcer leur cybersécurité nationale en comblant les failles réseau, en nettoyant les sites officiels dégradés et en sécurisant les infrastructures critiques vulnérables pour réduire le risque d'attaques potentiellement dévastatrices.

Après les pertes financières considérables subies par des entreprises et des particuliers, l'opération, qui s'est déroulée de juillet à novembre 2022, a permis de détecter, d'enquêter sur et de désorganiser des cybercriminels via des activités de répression coordonnées par le biais des plateformes, outils et réseaux d'INTERPOL, en étroite collaboration avec AFRIPOL.

CONCLUSION

La prise de conscience de nouveaux visages de l'insécurité nécessite également des approches plus modernes de la politique de défense et de sécurité. Cela plaide pour une certaine refonte de l'orientation même de cette politique de sécurité et de défense. Ces nouvelles dimensions de l'insécurité sont l'œuvre des acteurs intérieurs (acteurs armés : les organes étatiques chargés d'assurer la sécurité, les groupes armés intérieurs, les mouvements rebelles, etc.) et des acteurs extérieurs (Groupes armés étrangers, groupes terroristes, les armées étrangères, les sociétés multinationales du secteur minier, etc.).

Au fait, les nouveaux acteurs sécuritaires sont des secteurs-clés qui aujourd'hui, ont dépassé les frontières militaires pour devenir des préoccupations publiques. De nouveaux acteurs de la sécurité sont nés, à cause de l'émergence d'autres formes de menaces et de violences dans le monde et dans les communautés. Mais pour qu'une politique de sécurité et de défense soit efficace et efficiente, un préalable important est nécessaire : la démocratie en général, la démocratisation du secteur de la sécurité en particulier.

Il conviendrait que la gouvernance du secteur de la sécurité rame sur de nouvelles pistes afin d'éviter que l'Etat ne soit lui-même générateur de la violence et de l'insécurité, et pour permettre qu'il puisse contribuer à l'amélioration de la sécurité. Dans cette optique, de nouveaux modes de gouvernance du secteur de sécurité pourraient non seulement prévenir les abus pouvant engendrer la violence et l'insécurité, mais ils pourraient également exploiter ces appareils pour améliorer sensiblement la sécurité de tous. La réforme de la gouvernance sécuritaire devra porter tant sur le plan interne que sur le plan externe.

Pour faire face à un éventail croissant de cybermenaces et de défis, les gouvernements africains doivent adopter des stratégies de cybersécurité qui favorisent la collaboration et la confiance entre les acteurs civils et des secteurs de la sécurité et privé. La simple existence de cyber-stratégies nationales ou régionales n'est pas suffisante. Ce qui compte le plus, c'est leur conception, leur mise en œuvre et leur impact. Il existe toute une série de bonnes pratiques dans l'élaboration des stratégies en matière de cybersécurité et de sécurité nationale. Au minimum, les cyber-stratégies efficaces justifient leur nécessité, ce qu'il faut faire, quand il faut le faire, qui est responsable, et comment elles doivent être financées et mises en œuvre.

BIBLIOGRAPHIE

- ALLEN, N. et LENA KELLY, C., « Un déluge de répression numérique menace la sécurité africaine », in *Éclairage*, Centre d'études stratégiques de l'Afrique, 13 janvier 2022.
- BOGUI, J-J., « La cybercriminalité, menace pour le développement. Les escroqueries Internet en Côte d'Ivoire », in *Afrique contemporaine*, 2010/2, n° 234.
- Conseil de l'Europe, *État des signatures et ratifications du Traité 185*, 2020.

- Conseil de l'Europe, *L'état de la législation sur la cybercriminalité en Afrique - un aperçu*, 2015.
- Conseil de l'Europe, *The global state of cybercrime legislation 2013 – 2020 : A cursory overview*, 2020.
- Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel.
- CUSSON, M. et alii, *Traité de sécurité intérieure*, Hurtubise HMH, Montréal, 2007.
- du BOIS P., « Anciennes et nouvelles menaces : les enjeux de la sécurité en Europe », in *Relations internationales*, n°125, 2006.
- DUMOULIN, *Risques et menaces dans un monde en mutation*, Paris, 1992.
- FRANCIS, J-D., *Uniting Africa. Building Regional Peace and Security Systems*, Aldershot, Ashgate, 2007.
- <https://africacenter.org/fr/spotlight/lecons-dafrique-en-matiere-de-cyber-strategie>.
- <https://www.dw.com/fr/afrique-cybercriminalite/C3%A9/a-61251435>.
- <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2022/Une-operation-a-travers-le-continent-africain-permet-d-identifier-des-cybercriminels-et-les-infrastructures-virtuelles-a-risque>.
- <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique>.
- <https://www.interpol.int/fr/Infractions/Cybercriminalite/Operations-en-matiere-de-cybercriminalite/Operation-conjointe-de-lutte-contre-la-cybercriminalite-en-Afrique-AFJOC>.
- <https://www.vie-publique.fr/parole-dexpert/271196-afrique-le-defi-de-la-securite>.
- INTERPOL, *Rapport d'évaluation des cybermenaces en Afrique. Présentation des principales cybermenaces par le desk africain pour les opérations de lutte contre la cybercriminalité*, Mars 2023.
- LEWAL J., *Tactiques de sécurité*, Tome 1, Baudouin, Paris, 1883.
- MBELU BIOSHA, J-H., *Menaces sécuritaires en Afrique post guerre froide. Vers des nouvelles stratégies de riposte pour la stabilité et l'émergence de la République Démocratique du Congo*, Thèse de doctorat en SPA, FSSAP, UNIKIN, 2021.
- QUEMENER M. et FERRY J., *Cybercriminalité et défi mondial*, 2^{ème} édition, Ed. Economica, Paris, 2009.