Laboratoire Africain de
Recherches en Cyberstratégie

Former des cyberstratèges africains, un impératif !

DJIMGOU NGAMENI

François-Xavier

Résumé

Dans un contexte d'accélération de la transformation numérique en Afrique, la sécurité des systèmes d'information reste largement négligée, exposant le continent à une cybercriminalité croissante. Malgré une prise de conscience progressive, l'Afrique fait face à un déficit de professionnels qualifies en cybersécurité, estimé à plus de 112 000 postes non pourvus. Les formations actuelles, majoritairement axées sur les compétences techniques, ne suffisent plus face a l'évolution des menaces, notamment les cyberattaques étatiques. Il devient impératif de former des cyberstratèges africains capables d'intégrer une vision géopolitique et stratégique dans la défense du cyberespace africain et de ses intérêts.

Mots clés : Cybersécurité, Cyberstratégie, transformation numérique, Afrique, compétences.

Cybersecurity threats evolve rapidity, and without a well-trained workforce, organizations are exposed. It's not just about developing skills, but about building trust and providing continuous upskilling opportunities.

Dr Martin KOYABE,
Senior Manager & Technical lead
Global Forum of Cyber Expertise Africa.

23/09/2025

INTRODUCTION

Dans un contexte d'hyper connectivité à l'échelle mondiale, la transformation numérique de l'Afrique s'accélère, ouvrant des perspectives économiques et sociales inédites. Cependant, cette digitalisation croissante du continent s'opère encore selon une approche qui n'intègre pas dès la conception, le volet sécuritaire (le modèle dit *security by design*), approche aujourd'hui considérée comme dépassée. Ce qui n'est pas sans conséquences. Elle s'accompagne d'une augmentation rapide de la surface d'attaque, et par conséquent d'une cybercriminalité galopante en réaction à un accroissement spectaculaire des vulnérabilités structurelles. Bien qu'on observe une forte progression de la prise de conscience sur l'importance de la cybersécurité par différents acteurs en Afrique, un défi majeur persiste tout de même : le déficit alarmant de professionnels qualifiés pour assurer une protection et une défense efficaces des systèmes d'information du continent.

Selon une étude de l'organisation ISC2 datant de 2023, la pénurie de main-d'œuvre formée et compétente en cybersécurité en Afrique était estimée à environ 112.000 professionnels. Exacerbé par un ensemble de facteurs aggravants, ce déficit de compétences prend une dimension particulière sur le continent. On peut citer le faible niveau de sensibilisation des populations (y compris des décideurs malgré les avancées récentes), le manque de moyens financiers des PME pour former convenablement leur personnel, l'inadéquation de certains cursus de formation existants qui sont souvent calqués sur des modèles extérieurs et ne permettent pas de répondre efficacement aux enjeux locaux, la méconnaissance de l'ensemble du panorama des métiers de la cybersécurité, etc.

Pour y faire face, le continent africain voit fleurir des initiatives de formation en cybersécurité (cursus master, formations certifiantes, etc.), principalement axées sur les compétences et métiers d'experts techniques. Si cet effort de développement du capital humain manquant est louable, il reflète une vision dépassée de la menace, encore centrée sur la cybercriminalité [au sens de l'extension de la criminalité ordinaire dans le cyberespace]. Or, l'évolution du paysage cyber est marquée par une forte progression des attaques étatiques, exigeant des profils aux compétences non seulement techniques, mais aussi géopolitique et stratégique.

I. L'ÉMERGENCE DE LA FIGURE DU CYBERSTRATÈGE

Dans un contexte international marqué par la cyberconflictualité (opérations d'influence, menace sur les intérêts vitaux des États à travers des outils numériques), on a vu naître des profils nouveaux dans la protection et la défense de l'espace cybernétique d'un État. Parmi ces nouveaux profils on peut citer le cybercombattant[1], le cyberstratégiste, et enfin le cyberstratège, figure centrale de cyberdéfense sur laquelle nous entendons nous appesantir.

Imposé par l'émergence du cyberespace comme milieu stratégique et théâtre d'opérations militaire, ce nouveau profil, extrêmement exigeant en matière de socle de connaissances, d'aptitudes et de compétences, dépasse de loin l'expertise technique traditionnelle à laquelle nous sommes habitués.

En effet, le cyberstratège doit tout d'abord posséder une très solide culture technique du cyberespace (connaissance des architectures réseaux et systèmes d'information, du fonctionnement des systèmes d'information d'infrastructures critiques, technologies émergentes, types de cyberattaques, modes opératoires des acteurs malveillants et stratégies de défense, etc.) De plus, il doit avoir une fine compréhension des enjeux géopolitiques, des relations internationales, des rivalités de pouvoir et dynamiques de puissance mondiale (identifier les acteurs étatiques et non-étatiques dans le cyberespace, leurs motivations, leurs capacités cybernétiques, leurs alliances, etc.) ; du droit international (connaître les traités, conventions, initiatives internationales visant à réguler ce nouveau domaine) ; et des doctrines stratégiques adaptées au cyberespace.

Mais ce n'est pas tout! Être cyberstratège c'est surtout, en qualité de spécialiste et praticien de la cyberstratégie, avoir la capacité d'appliquer les principes de la stratégie à l'environnement cybernétique. Cela suppose la ferme connaissance d'une doctrine en la matière qui précise par exemple, la théorie sur la dissuasion cybernétique en vigueur dans son pays (comment dissuader un adversaire de mener des cyberattaques majeures ? Quels sont les

[1] Le cybercombattant est un spécialiste de la cybersécurité au service des armées, de la Gendarmerie ou d'autres services publics, en charge la lutte informatique offensive (mandater par l'autorité politique pour attaquer les systèmes informatiques d'un adversaire) ou défensive (de défendre les systèmes informatiques des armées et des entreprises des secteurs sensibles).

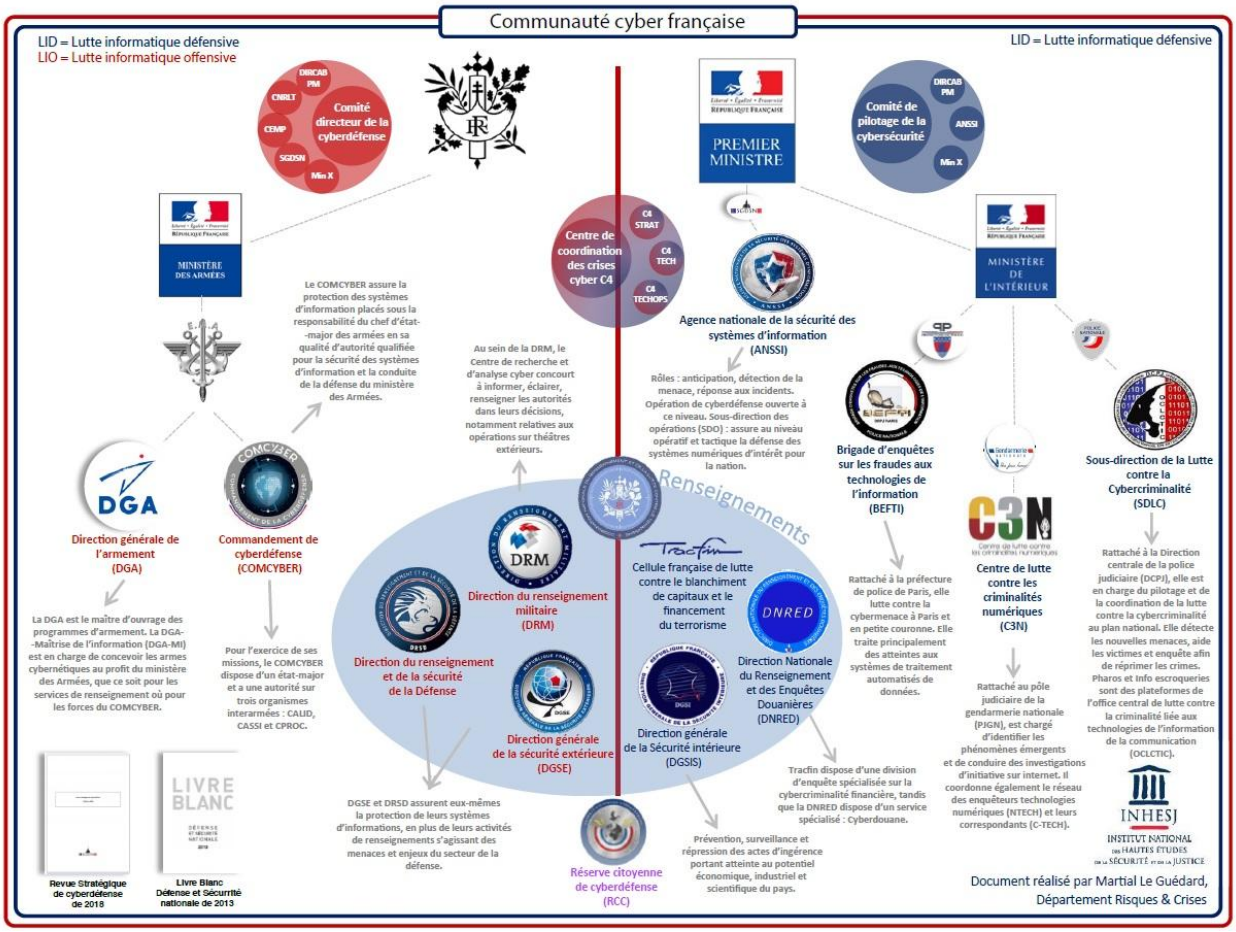
mécanismes de dissuasion crédibles dans le cyberespace? etc.), les mécanismes d'attribution technique, politique ou diplomatique d'une attaque à un État, la démarche de qualification des cyberattaques étatiques et le choix des moyens de riposte selon le niveau de gravité, etc.

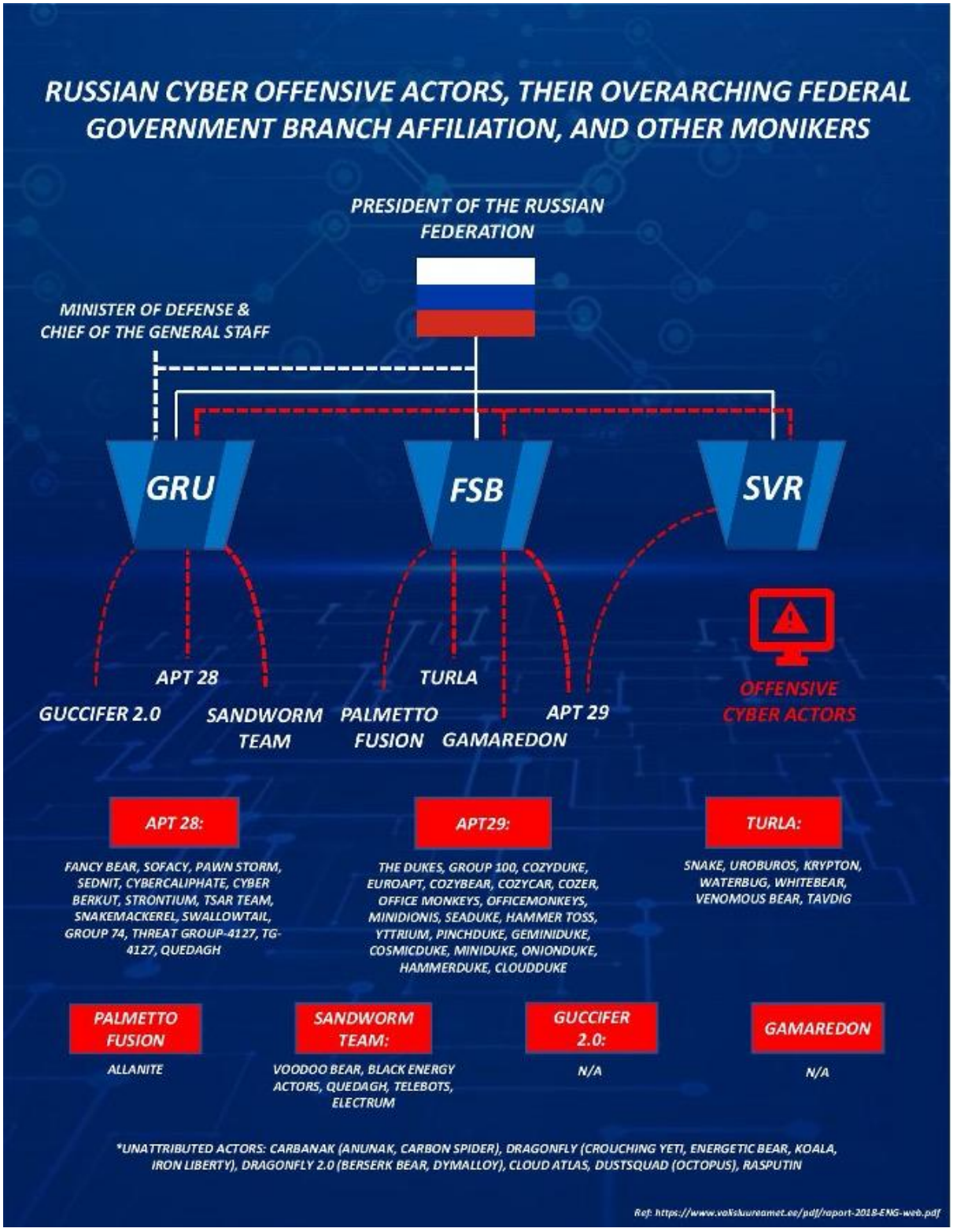
Naturellement curieux, intellectuellement rigoureux avec un esprit à la fois ouvert et critique, cet expert de haut vol doit également être familier avec l'analyse prospective ainsi que l'art du renseignement en rapport avec le cyberespace (maîtriser les concepts de renseignement d'origine cyber vs renseignement d'intérêt cyber par exemple). Il doit comprendre les risques d'escalade d'un incident cybernétique vers un conflit plus large, maîtriser les mécanismes pour désamorcer les tensions, être au fait des différentes modalités d'application du droit des conflits armés et du droit international humanitaire dans le cyberespace. Si l'efficacité d'une cyberstratégie repose nécessairement sur une équipe pluridisciplinaire (composée notamment de cybercombattants et cyberstratégistes[2]), où chacun apporte ses compétences complémentaires, le cyberstratège est bien ce chef d'orchestre capable de coordonner l'ensemble du dispositif avec méthode et efficience.

Profil atypique et sensible, leader éprouvé au passé militaire (du moins, la plupart du temps), on le retrouve à la tête de diverses entités dans l'architecture organisationnelle de protection et de défense du cyberespace d'un État (il peut s'agir selon le pays d'agence gouvernementale spécialisée, d'unité cyber des armées ou des services de renseignement, comme l'illustrent les images ci-dessous). Prenons le cas des États Unis. Paul MIKI NAKASONE, général quatre étoiles de *l'United States Army* et actuel commandant de l'United States Cyber Command, est un exemple typique de cyberstratège.

[2] Un cyberstratégiste est un penseur spécialisé dans la cyberstratégie. Son rôle consiste à analyser le contexte des rivalités cybernétiques pour concevoir les cadres théoriques et les lignes directrices doctrinales qui structurent la posture stratégique et la gestion des rapports de force d'une entité nationale dans l'environnement numérique.


U.S. Cyber Command
Components
U.S. Army Cyber Command
Headquarters: Fort Gordon, Georgia
U.S. Fleet Cyber Command
Headquarters: Fort Meade, Maryland
Air Forces Cyber
Headquarters: Joint Base San Antonio, Texas
Marine Corps Forces Cyberspace Command
Headquarters: Fort Meade, Maryland


Communauté cyber française
LID = Lutte informatique défensive
LIO = Lutte informatique offensive
LID = Lutte informatique défensive
Comité directeur de la cyberdéfense
Comité de pilotage de la cybersécurité
PREMIER MINISTRE
MINISTÈRE DES ARMÉES
MINISTÈRE DE L'INTÉRIEUR
Centre de coordination des crises cyber C4
Agence nationale de la sécurité des systèmes d'information (ANSSI)
Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cyberdéfense ouverte à ce niveau. Sous-direction des opérations (SDO) : assure au niveau opératif et tactique la défense des systèmes numériques d'intérêt pour la nation.
Le COMCYBER assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information et la conduite de la défense du ministère des Armées.
Au sein de la DRM, le Centre de recherche et d'analyse cyber concourt à informer, éclairer, renseigner les autorités dans leurs décisions, notamment relatives aux opérations sur théâtres extérieurs.
Renseignements
Direction générale de l'armement (DGA)
Commandement de cyberdéfense (COMCYBER)
La DGA est le maître d'ouvrage des programmes d'armement. La DGA-Maîtrise de l'information (DGA-MI) est en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement où pour les forces du COMCYBER.
Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées : CALID, CASSI et CPROC.
Direction du renseignement militaire (DRM)
Direction du renseignement et de la sécurité de la Défense
Direction générale de la sécurité extérieure (DGSE)
DGSE et DRSD assurent eux-mêmes la protection de leurs systèmes d'informations, en plus de leurs activités de renseignements s'agissant des menaces et enjeux du secteur de la défense.
Tracfin
Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme
DNRED
Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)
Direction générale de la Sécurité intérieure (DGSIS)
Tracfin dispose d'une division d'enquête spécialisée sur la cybercriminalité financière, tandis que la DNRED dispose d'un service spécialisé : Cyberdouane.
Prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique du pays.
Réserve citoyenne de cyberdéfense (RCC)
Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)
Rattaché à la préfecture de police de Paris, elle lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des atteintes aux systèmes de traitement automatisés de données.
C3N
Centre de lutte contre les criminalités numériques (C3N)
Rattaché au pôle judiciaire de la gendarmerie nationale (PJGN), est chargé d'identifier les phénomènes émergents et de conduire des investigations d'initiative sur internet. Il coordonne également le réseau des enquêteurs technologies numériques (NTECH) et leurs correspondants (C-TECH).
Sous-direction de la Lutte contre la Cybercriminalité (SDLC)
Rattaché à la Direction centrale de la police judiciaire (DCPJ), elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes. Pharos et Info escroqueries sont des plateformes de l'office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC).
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE
LIVRE BLANC
Revue Stratégique de cyberdéfense de 2018
Livre Blanc Défense et Sécurité nationale de 2013
Document réalisé par Martial Le Guédard, Département Risques & Crises


RUSSIAN CYBER OFFENSIVE ACTORS, THEIR OVERARCHING FEDERAL GOVERNMENT BRANCH AFFILIATION, AND OTHER MONIKERS
PRESIDENT OF THE RUSSIAN FEDERATION
MINISTER OF DEFENSE & CHIEF OF THE GENERAL STAFF
GRU
FSB
SVR
APT 28
GUCCIFER 2.0
SANDWORM TEAM
TURLA
PALMETTO FUSION
APT 29
GAMAREDON
OFFENSIVE CYBER ACTORS
APT 28:
FANCY BEAR, SOFACY, PAWN STORM, SEDNIT, CYBERCALIPHATE, CYBER BERKUT, STRONTIUM, TSAR TEAM, SNAKEMACKEREL, SWALLOWTAIL, GROUP 74, THREAT GROUP-4127, TG-4127, QUEDAGH
APT29:
THE DUKES, GROUP 100, COZYDUKE, EUROAPT, COZYBEAR, COZYCAR, COZER, OFFICE MONKEYS, OFFICEMONKEYS, MINIDIONIS, SEADUKE, HAMMER TOSS, YTTRIUM, PINCHDUKE, GEMINIDUKE, COSMICDUKE, MINIDUKE, ONIONDUKE, HAMMERDUKE, CLOUDDUKE
TURLA:
SNAKE, UROBUROS, KRYPTON, WATERBUG, WHITEBEAR, VENOMOUS BEAR, TAVDIG
PALMETTO FUSION
ALLANITE
SANDWORM TEAM:
VOODOO BEAR, BLACK ENERGY ACTORS, QUEDAGH, TELEBOTS, ELECTRUM
GUCCIFER 2.0:
N/A
GAMAREDON
N/A
*UNATTRIBUTED ACTORS: CARBANAK (ANUNAK, CARBON SPIDER), DRAGONFLY (CROUCHING YETI, ENERGETIC BEAR, KOALA, IRON LIBERTY), DRAGONFLY 2.0 (BERSERK BEAR, DYMALLOY), CLOUD ATLAS, DUSTSQUAD (OCTOPUS), RASPUTIN
Ref: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

II. LE CYBERSTRATÈGE AFRICAIN

Comme aux Etats Unis, ce profil existe depuis plusieurs années dans les pays ayant une ambition de cyber puissance, conscient des enjeux et des rapports de force dans le cyberespace, avec une culture des opérations cyber offensives suffisamment développée. La Russie, la Chine, la France, le Royaume Uni, Israël, l'Iran, l'Australie, etc. en font certainement partie. Il s'est d'ailleurs récemment produit un événement assez inédit et fortement illustratif de notre propos. Le 29 Avril 2025, la diplomatie française a annoncé que la France attribue officiellement une série de cyberattaques contre elle à la fédération de Russie, notamment à son service de renseignement militaire (le GRU et son groupe affilié APT28)[1]. ***Cette attribution politico-diplomatique officielle est tout de même une première mondiale en matière de cyberstratégie***. Il est évident que des cyberstratèges ont été à l'œuvre de part et d'autre, aussi bien côté offensif (cibler et attaquer les intérêts français dans le cyberespace) que défensif (répondre et attribuer les attaques à la Russie), dans un contexte stratégique difficile entre les belligérants sur fond de guerre russo-ukrainienne.

La plupart des États africains n'étant pas inscrits dans cette démarche d'affrontement entre États dans l'espace cybernétique, il est logique qu'on ait du mal à trouver ce type de profil sur le continent. Des exemples comme le Col. David KANAMUGIRE, Directeur de l'Autorité Nationale rwandaise de cybersécurité (directement rattachée à la présidence), ou encore le Colonel-major Guelpetchin Ouattara[2], officier supérieur de la gendarmerie ivoirienne a la tête de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'information) depuis janvier 2025, font partie des rares exceptions de cyberstratèges africains.

Pourtant, comme le souligne le LARC - Laboratoire Africain de Recherche en Cyberstratégie dans différentes publications, le continent de Kwame Nkrumah est devenu une cible privilégiée pour les cyberpuissances et autres acteurs malveillants dans le cyberespace en raison de : ses vulnérabilités structurelles, ses manquements organisationnels, l'augmentation de la surface d'attaque dûe à une constante progression de la connectivité sur le continent, son importance géopolitique croissante, ainsi que son potentiel économique.

Pour pouvoir répondre efficacement à ces nouvelles formes de menaces, l'Afrique, au-delà des experts techniques, doit urgemment se doter de cyberstratèges outillés pour appréhender la complexité de ces nouveaux enjeux. D'où, la nécessité au regard des tendances

et perspectives d'évolution toujours aussi conflictogènes du cyberespace, d'en former au maximum. Car nos Etats en auront grandement besoin dans les années à venir. Le cyberstratège africain est un architecte de la cyberdéfense nationale ou continentale capable de :

- ☑ Analyser le cyberespace africain dans sa spécificité, en identifiant les acteurs, menaces et vulnérabilités propres au continent.
- ☑ Définir des stratégies de cybersécurité adaptées aux réalités africaines, en tenant compte des ressources limitées, des priorités nationales, des alliances et partenariats stratégiques de l'Afrique, etc.
- ☑ Anticiper les cybermenaces et les évolutions technologiques afin de préparer des réponses adéquates.
- ☑ Dialoguer avec les décideurs politiques pour traduire les enjeux cyber en politiques publiques efficaces, en résonance avec le contexte géopolitique mondial.
- ☑ Coopérer avec les partenaires internationaux tout en défendant les intérêts souverains africains dans le cyberespace.

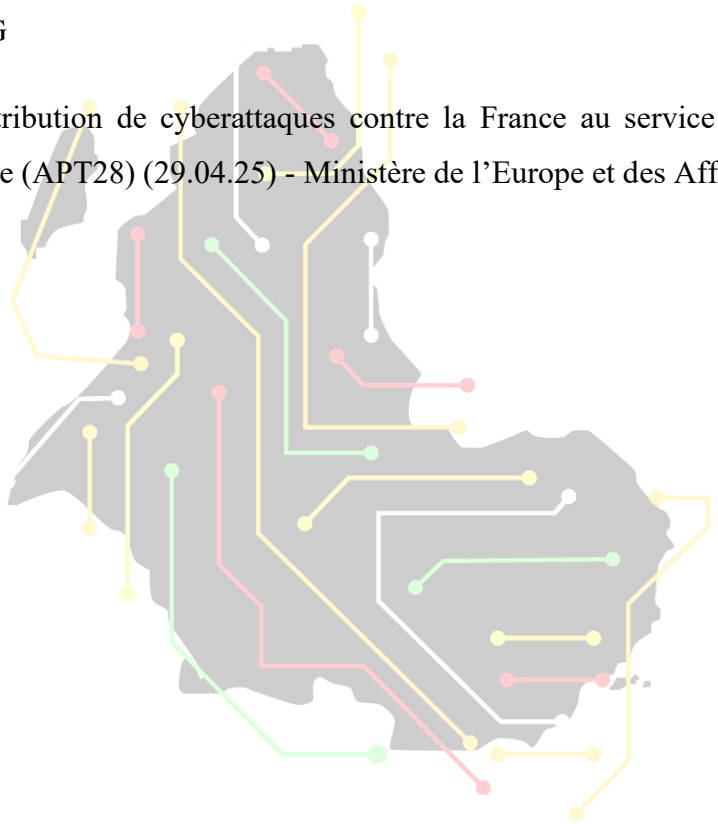
Face à cet état de fait, l'Afrique doit former des profils et développer les compétences adéquates pour organiser efficacement sa gouvernance. L'émergence d'une génération de cyberstratèges africains, ancrés dans les réalités du continent et formés aux enjeux spécifiques de son cyberespace, est une nécessité urgente pour garantir la souveraineté numérique et la sécurité d'une Afrique connectée dans le 21e siècle. Investir dans la formation de ces profils stratégiques est un impératif pour un avenir numérique africain maîtrisé et sécurisé. Fort de cela, le LARC lancera dès 2026 un Programme de certification en cyberstratégie africaine. Cette formation encore inédite sur le continent s'inscrit dans le cadre de l'initiative **« 100.000 cyberveillleurs africains »,** démarche plus globale visant à résorber la pénurie chronique de professionnels qualifiés sur les métiers de protection et défense du cyberespace africain.

Références

Col Kanamugire to head NCSA, Lt. Col Ngabo for RSA as ACP Nkuranga steers NISS external | IGIHE

Qui est Guelpetchin Ouattara, le premier Directeur général de l'ANSSI de Côte d'Ivoire ? – CIOMAG

Russie – Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) (29.04.25) - Ministère de l'Europe et des Affaires étrangères



À propos de l'Auteur :

DJIMGOU NGAMENI est le fondateur du LARC et CEO de RHOPEN LABS. Auteur de plusieurs ouvrages, il est également Conférencier, Consultant en cybersécurité/cyberdéfense, et conduit des travaux sur la cyberstratégie en Afrique.

À propos du LARC :

Le LARC (Laboratoire Africain de Recherches en Cyberstratégie) est un cadre de réflexion, créé par votre serviteur et regroupant des chercheurs pluridisciplinaires, avec pour mission de décrypter, d'analyser et d'anticiper les enjeux de demain dans le cyberespace africain.

Pour soutenir les activités du LARC ou y contribuer par vos propres publications, visitez notre site web : https://www.larc.africa

Pour citer cet article :

Djimgou Ngameni, « Former des cyberstratèges africains, un impératif ! », Note N° 19 — LARC, Septembre 2025.