Laboratoire Africain de
Recherches en Cyberstratégie

L'Afrique peut devenir une Cyberpuissance

Résumé

Les discours selon lesquels l'Afrique serait retardée du point de vue technologique peuvent aujourd'hui trouver des arguments a contrario. L'avènement des critères mondiaux d'indice et d'évaluation de niveau cyber permettent à tous de se mettre à niveau. Comme tous les autres, l'Afrique elle aussi peut devenir une cyberpuissance ! Au-delà d'acquérir une souveraineté numérique, elle peut aujourd'hui aspirer à être puissante numériquement parlant. Mais la grande question demeure, comment l'Afrique peut-elle réussir à devenir une cyberpuissance aujourd'hui ? Ce qu'il faudrait savoir au préalable, c'est que le continent dispose de plusieurs facteurs que d'aucuns jugeraient a priori désavantageux, mais qui pris sous une considération différente, deviendraient des avantages. La présente réflexion tente une analyse profonde sur la notion de cyberpuissance. Partant d'une définition et d'un rapprochement entre le concept de puissance et le continent africain, ressortent les différents facteurs indiquant la cyberpuissance d'un Etat. L'objectif étant, de démontrer par des voies et moyens à mettre en jeu, comment l'Afrique a toutes ses chances de devenir elle aussi une cyberpuissance. La mise en pratique demeurant…

Mots clés : puissance, cyberpuissance, évaluation cyber, Afrique, émergence, hégémonie, démarche africaine.

Par François-Xavier Djimgou Ngameni

Extrait du livre à paraître :

Cyberstratégie Africaine, Tome 2

Introduction au concept de puissance

La puissance est un concept qui au fil du temps a fait l'objet de beaucoup de travaux et de débats entre philosophes, scientifiques, militaires, etc. Évacuons d'abord l'idée de puissance exprimée comme capacité de la mise en mouvement décrite par les lois de la physique, qui sort du cadre [géopolitique] dans lequel se déploie notre analyse.

Dans ce cadre, le concept de puissance est généralement associé aux notions d'action, de potentiel d'action et au pouvoir (dont il se distingue pourtant). On peut aussi relever l'idée préconçue selon laquelle pour un pays, la puissance se mesure nécessairement dans sa capacité à exercer des actions importantes et à plier les autres pays à ses volontés en les influençant. C'est une perception qui limite l'étendue de ce concept, et entre d'ailleurs en rupture avec la vision du maître chinois Sun tzu qui dans son célèbre traité "l'art de la guerre" nous enseigne que « par le mot puissance il ne faut pas entendre domination, mais la faculté qui fait qu'on peut réduire en acte tout ce qu'on se propose ». Face à cette apparente contradiction, Jean-François Bianchi soutient que « la puissance n'est donc pas un absolu, mais un rapport très relatif, tout autant psychologique, cognitif, que matériel à autrui. […] Elle s'évalue en forces, donc en capacités matérielles comme immatérielles, et se compare dans des rapports de force, qui prédéterminent une part substantielle des effets espérés »

De façon classique, la puissance d'un pays passe par trois voies essentielles : la puissance militaire, qui depuis toujours permet de faire valoir les intérêts d'une nation. La puissance économique, qui est aujourd'hui le théâtre de toutes les confrontations des nations contemporaines avec un consensus des spécialistes en géopolitique sur le fait que la guerre militaire a fait place à la guerre économique, et les armées se transformant en conséquence. Ces deux voies de la puissance constituent le hard power, c'est-à-dire la capacité d'imposer sa volonté (par la contrainte, la force) en pliant celle de l'autre. La troisième voie classique est la puissance culturelle (concept de soft power développé par le professeur américain Joseph S. Nye) qui utilise comme vecteurs la langue, les cultures ou encore la religion pour façonner les volontés et consolider sa position internationale.

Relevons que depuis 2004, la diplomate américaine Suzanne Nosel a théorisé une nouvelle catégorie de puissance dite smart power, entendue globalement comme synthèse et combinaison entre le hard power (capacité à contraindre) et le soft power (capacité à inciter, à persuader). Le concept a d'ailleurs été officiellement repris comme nouvelle matrice des relations internationales par l'administration américaine sous Obama, clairement illustré dans un discours prononcé en 2009 par Hillary Clinton alors secrétaire d'État. C'est à cette nouvelle catégorie que certains spécialistes classent désormais la guerre économique.

I. Le rapport de l'Afrique à la notion de puissance

La notion de durabilité est une notion difficile à cerner. Elle présente des nuances Contrairement aux signes de faiblesse et d'impuissance que l'Afrique d'aujourd'hui peut laisser transparaître, le concept de puissance n'est pas étranger à sa culture et à son histoire pluriséculaire (notamment la partie qui a très souvent été occultée). En témoigne par exemple la littérature de plus en plus abondante sur le règne des pharaons tels que THOUTMOSIS III ou encore RAMSES II, dont on constate qu'ils avaient déjà une connaissance pratique de la puissance classique (aussi bien militaire, économique que culturelle). Décrit par les égyptologues comme des rois guerriers, on sait désormais qu'ils furent d'extraordinaires conquérants au service de la restauration de l'empire Egyptien, démantelé par des envahisseurs (les Hyksos) lors des règnes de leurs prédécesseurs. Une analyse rigoureuse de leurs épopées permet très rapidement de se rendre compte à la fois de leur ambition de grandeur, leur génie militaire et leur

stratégie de puissance, nourries par la volonté de repousser les envahisseurs au plus loin et de consolider le rayonnement de la civilisation pharaonique.

En Egypte antique, cette notion de puissance revêt une connotation particulière, symbolisée par la déesse lionne Sekhmet (ce nom signifie d'ailleurs « la puissante »). D'après la mythologie, il s'agit de la divinité qui accompagne l'armée du pharaon sur les champs de bataille afin de l'aider à terrasser les ennemis de l'empire, du moment où elle se bat pour une cause noble et juste (la Maât). Même si Sekhmet représente bien plus que la force et la puissance (personnage ambivalent, elle incarne aussi la bienveillance, la douceur, la guérison), sa figure de divinité féline a été régulièrement reprise au cours de l'histoire pour symboliser ce concept.

Quand on observe la place de l'Afrique dans le monde, la façon dont elle est perçue, les rapports de force entre les grands blocs idéologiques qui s'affrontent sur le continent (Chine, Russie, Etats-Unis, France, Turquie, etc.), il y a suffisamment de causes nobles aujourd'hui justifiant que les africains se mobilisent à nouveau autour d'une idée de reconquête de leur espace vitale, d'autodétermination [tel que le font déjà plusieurs mouvements de la société civile sur le continent].

Ainsi, il est question de renouer et de se réapproprier cette expérience historique millénaire de volonté, d'ambition de grandeur et de stratégie de puissance. C'est à partir de cet héritage que l'Afrique pourra concevoir une nouvelle approche de ce concept qui soit authentique et adaptée à notre temps, donc adaptable aux enjeux de l'heure et aux nouveaux théâtres tel que l'est aujourd'hui le cyberespace. Car comme aime à le rappeler Christian Harbulot [directeur de l'Ecole de Guerre Économique], « la matrice de construction de la puissance est propre à chaque pays, et c'est un élément fortement différenciateur d'un pays à l'autre ». La même réflexion peut être faite à l'échelle continentale.

II. Le concept de cyberpuissance

Dans les langues de culture européenne, le verbe disposer a plusieurs sens. Un de ces sens Avec l'émergence fulgurante du numérique, de la société de l'information, du monde immatériel, le concept de puissance tend à évoluer ou à se reconstruire sur la base de nouveaux paramètres, de nouveaux attributs. On constate que le cyberespace, par sa nature et ses propriétés, a un impact concret sur l'expression de la puissance dans ses formes classiques. Au regard des capacités extraordinaires que disposent les technologies numériques pour influencer les habitudes (de consommations par exemple), véhiculer une idéologie et des valeurs, le numérique est souvent rangé dans la catégorie du soft power.

Cependant, le cyberespace est aussi un espace d'échange et de compétition économique par excellence, sur lequel repose presque entièrement le modèle d'affaires des géants du net (GAFAM, BATX, NATU, etc.). Ce sont désormais les entreprises les plus riches du monde en valeur boursière ! A travers sa structuration en couches (physique, logiciel et sémantique) et la prédominance des technologies américaines sur chacune d'elle (au niveau global), c'est aussi devenu un champ d'affrontement économique. Car les autres puissances ont commencé à développer leurs propres technologies d'abord pour échapper à la dépendance étatsunienne, puis pour conquérir les nouvelles parts de marché dans le monde (au détriment des acteurs américains). L'affaire Huawei, objet de guerre économique (et stratégique) avérée entre Chine et Etats-Unis, est un cas d'école en la matière.

De même, le cyberespace a été reconnu comme « milieu stratégique » par l'OTAN depuis 2016, le consacrant de fait comme un nouveau domaine militaire, un théâtre d'affrontement, un champ de combat. On a ainsi vu proliférer les cyberarmes au cours de la dernière décennie, avec jusqu'à 120 pays

dans le monde en date de 2012 qui selon plusieurs études auraient développé des capacités de lutte informatique offensive. Ces armes numériques ont pour cible dans les pays considérés comme ennemi ce qu'il convient aujourd'hui d'appeler des OIV (Opérateurs d'Importance Vital), entendu comme toute organisation identifiée par l'État comme ayant des activités indispensables ou dangereuses pour la population. D'où l'émergence des concepts de cyberespionnage, de cyberdéfense, de cyber-conflictualité, de cyberguerre et de cyber dans la guerre (utilisation des technologies numériques comme armes supplémentaires lors d'une opération militaire : cas de l'opération Russe en Géorgie en 2008).

Ces implications dans les domaines économique et stratégique inscrivent les technologies numériques dans la catégorie du hard power aussi ! Le cyberespace, par sa nature complexe, traverse ainsi le panorama de toutes les voies de la puissance classique tout en créant une autre… On voit donc apparaître une nouvelle forme de puissance basée sur le cyberespace : la cyberpuissance ! Comme nous venons de le constater, cette cyberpuissance peut se manifester en soft ou en hard power, rendant compte du caractère hybride du cyberespace. Peut-elle aussi exister par elle-même, c'est-à-dire en dehors des autres voies de la puissance classique ?

D'après Olivier Kempf, "il est raisonnable de penser qu'il existe une certaine corrélation entre le niveau de puissance classique (économique, technologique et militaire) et le niveau de cyberpuissance ". D'aucuns pensent que le cyberespace peut permettre de consolider, d'amplifier, ou de catalyser la puissance d'un État (outil d'accroissement de la puissance). D'autres, au regard du caractère opaque et ubiquitaire du cyberespace qui rend difficile l'attribution d'une cyber-agression, parlent plutôt d'un égalisateur de puissance qui modifie le rapport du faible au fort. En ce sens que l'avantage stratégique revenant à l'attaquant, un « Etat faible » ou même un acteur non étatique peut [par les moyens cyber] agresser un « Etat fort » sans se faire inquiéter, vu qu'il est très difficile de remonter avec certitude à la source.

À ce stade, une série de questions se posent d'elles-mêmes : comment devient-on une cyberpuissance ? Quels sont les critères et comment sont-ils mesurés ? Sur la base de ces critères, quels pays sont aujourd'hui considérés comme des cyberpuissances ? Et la question la plus importante : l'Afrique peut-elle devenir une cyberpuissance ?

III. Critères d'évaluation des cyberpuissances

Il existe aujourd'hui plusieurs approches permettant, sur la base d'indicateurs et de critères divers, de mesurer le niveau de maturité d'un pays en matière de cybersécurité et de cyberdéfense. Pendant que certains outils comme l'étude GCI (Global Cybersecurity Index), le CRI (Cyber Readiness Index) et plus récemment le NCPI (National Cyber Power Index) sont parmi les plus connus proposés par des organisations, d'autres types d'approches sont à l'initiative des chercheurs et théoriciens qui eux aussi essayent de comprendre cette notion de cyberpuissance, parfois avec des nuances dans le choix des critères.

III.1. L'Indice Mondial de Cybersécurité

Le GCI, Indice Mondial de Cybersécurité, a été mis en place par L'Union Internationale des Télécommunications (UIT) qui est un démembrement technique de l'ONU en matière de télécommunication. Il s'agit d'une étude annuelle qui mesure le niveau de développement de chaque pays participant (134 pays pour 2018) en matière de cybersécurité, en évaluant leur niveau d'engagement sur la base de 25 indicateurs réparties dans les cinq domaines d'activités suivant :

- Le cadre juridique (ensemble de mesures fondées sur l'existence d'institutions et de cadres juridiques traitant de la cybersécurité et de la cybercriminalité),
- Les mesures techniques (ensemble de mesures fondées sur l'existence d'institutions et de cadres techniques traitant de la cybersécurité),
- Les structures organisationnelles (ensemble de mesures fondées sur l'existence d'institutions de coordination des politiques et de stratégies de développement de la cybersécurité au niveau national),
- Le renforcement des capacités (ensemble de mesures fondées sur l'existence de programmes de recherche et développement, d'éducation et de formation, de professionnels certifiés et d'organismes du secteur public favorisant le renforcement des capacités),
- La coopération internationale (ensemble de mesures fondées sur l'existence de partenariats, de cadres de coopération et des réseaux de partage d'informations).

L'objectif est de fournir aux pays la motivation adéquate afin d'intensifier leurs efforts en matière de cybersécurité, et d'encourager une culture mondiale de la cybersécurité en l'intégrant au centre même de la transformation numérique.

D'après le dernier rapport d'étude datant de 2018, les cinq premiers pays du classement (ayant un meilleur indice de cybersécurité) sont dans l'ordre : La grande Bretagne, les Etats-Unis, la France, la Lituanie et l'Estonie. Occupant le premier rang dans leur région respective, la Russie et la Chine sont respectivement en 26ème et 27ème position au niveau mondial. L'analyse de ce résultat est intéressante dans notre contexte. A priori, on peut être fondé à penser que les premiers pays du classement GCI seraient aussi les premières puissances numériques mondiales. Est-ce donc à dire que la Lituanie est une cyberpuissance supérieure à la Chine ou de la Russie au regard de leur écart dans ce classement ? L'actualité des rapports de force documentée sur l'échiquier cyber nous pousse quand même à en douter. En supposant que tous les pays participants ont sincèrement répondu au questionnaire d'enquête (ce dont il ne serait pas absurde de douter aussi), on peut donc tirer un double enseignement de ce résultat d'étude :

1. Les indicateurs et les domaines choisis ne sont pas suffisants comme critères pour évaluer une cyberpuissance.
2. Avoir un bon niveau de préparation en matière de cybersécurité et de lutte contre la cybercriminalité ne fait pas automatiquement d'un pays une cyberpuissance, même si ça y contribue grandement.

III.2. L'Indice de Préparation Cyber

Menée par le *Potomac Institute for Policy Studies*, centre de réflexion américain sous la coordination de Melissa Hathaway, l'indice de préparation cyber est un outil méthodologique articulé autour de 7 piliers. Il permet d'évaluer l'engagement et la capacité d'un pays à protéger ses infrastructures et ses services numériques nationaux dont dépendent son avenir en matière de croissance économique et de sécurité nationale. Cet outil s'inspire de l'étude GCI de l'UIT tout en essayant de la compléter et de la perfectionner, notamment dans l'approche de mesure et d'appréciation des critères d'évaluation. Le CRI sort de la logique de classement des pays sur la base d'un indice quantifiable, vers une logique de niveau de maturité cyber et de capacité des états à défendre leur cyberespace. Au-delà de la cybersécurité, cet outil, en mettant un accent particulier sur le lien entre la transformation numérique, la croissance économique et la sécurité des états, évalue aussi le dispositif de cyberdéfense.

Les sept critères évalués sont les suivants :

- La stratégie nationale : De l'aveu même des auteurs, le premier et le plus important élément qui indique l'état de préparation d'un pays en matière de cybers est l'articulation et la publication d'une stratégie nationale de cybers, qui aligne la vision économique du pays sur ses impératifs de sécurité nationale.
- La réponse aux incidents : ce second critère, qui indique l'état de préparation d'un pays en matière de cybersécurité, consiste à établir et à maintenir une capacité nationale efficace de réaction aux incidents.
- La cybercriminalité et l'application des lois : Il s'agit de l'engagement d'un pays à protéger sa société contre la cybercriminalité, entendu comme menace qui transcende les frontières nationales et nécessite donc des solutions transnationales. La cybercriminalité est perçue dans cette étude comme une forme de taxe sur la croissance économique des pays. La combattre représente ainsi un investissement !
- Le partage des informations : Ce critère mesure la capacité d'un Etat à établir et à maintenir des mécanismes de partage d'informations qui permettent l'échange de renseignements et/ou d'informations exploitables entre partenaires, aussi bien étatiques que des secteurs industriels.
- L'investissement dans la recherche et le développement (R&D) : Il s'agit ici d'ériger au rang de priorité nationale, l'investissement dans la recherche fondamentale et appliquée en matière de cybersécurité et dans les initiatives TIC en général. Car l'innovation en matière de R&D sur la cybersécurité contribuera à renforcer la confiance, la sécurité et la résilience de nos sociétés hyper connectées.
- La diplomatie et le commerce : Le sixième critère est démontré par l'engagement d'un pays à inscrire les questions relatives au cyberespace dans l'agenda de sa politique étrangère (cyber-diplomatie).
- La défense et la réponse aux crises : Ce septième et dernier élément mesure la capacité des forces armées nationales d'un pays et/ou de l'agence de défense correspondante à défendre le pays contre les cyber-menaces et/ou cyber-agressions sur ses intérêts de souveraineté et sa sécurité nationale.

Vous l'aurez constaté, contrairement à l'Indice Mondial de Cybersécurité (GCI), l'Indice de Préparation Cyber (CRI) dépasse le simple cadre de la cybersécurité pour insister sur sa corrélation avec le développement économique et la sécurité nationale d'un pays. Ce qui est à la fois intéressant et surprenant est que d'après la grille d'évaluation CRI (cf. image 1), le rapport de 2015 indiquait qu'aucun pays du monde n'avait encore suffisamment développé l'ensemble des critères [évoqués ci-dessus] pour être considéré comme "Cyber Ready". Quelques-uns le seraient-ils aujourd'hui ? Là encore, même si on peut reconnaître la rigueur des indicateurs et de l'analyse, se pose à nouveau la question sur la sincérité des réponses fournies par les pays participants.

III.3. L'Indice National de Cyberpuissance

Inspiré de tous les précédents outils d'étude et d'analyse du dispositif cyber d'un pays (notamment les deux que nous venons d'explorer), l'Indice National de Cyberpuissance (NCPI) a pour objectif principal de fournir un outil méthodologique plus affiné que les indices existants, permettant de mesurer la puissance cyber d'un pays. L'étude a été menée par le centre de recherche américain Belfer Center for Science and International Affairs, et rendue publique dans un rapport en Septembre 2020.

D'après le NCPI 2020, un État peut être considéré comme une cyberpuissance lorsqu'il fait montre de son intention d'utiliser les moyens cyber pour atteindre ses objectifs stratégiques nationaux, et détient les capacités de pouvoir effectivement les réaliser. L'étude a identifié sept principaux objectifs nationaux que les pays peuvent poursuivre par l'utilisation des moyens cybernétiques, parmi lesquels :

- Surveiller et contrôler les groupes (politiques, idéologiques, etc.) nationaux ;
- Renforcer et améliorer les capacités cyber-défensives nationales ;
- Contrôler et manipuler l'environnement de l'information ;
- Collecter des renseignements dans les pays étrangers pour la sécurité nationale ;
- Gain commercial ou renforcement de la croissance de l'industrie nationale ;
- Détruire ou désactiver l'infrastructure et les capacités d'un adversaire (grâce au développement des capacités cyber-offensives) ;
- Définir des normes internationales et des normes techniques en matière de numérique.

L'intention d'un État ici se manifeste par l'existence d'une cyberstratégie nationale, d'une rhétorique en la matière, ainsi que des opérations dans le cyberespace (cyberattaques) qui lui sont attribués à tort ou à raison, ce qui de toute façon démontre la reconnaissance de ses capacités par d'autres pays. Ainsi, le NCPI mesure le niveau d'intention et de capacités réelles d'un pays à utiliser les moyens cybernétiques pour atteindre ces objectifs clefs. Selon ces critères et cette méthodologie, sont considérés comme cyberpuissance les pays ayant le niveau d'intention et les capacités les plus élevées (mesuré par une vingtaine d'indicateurs combinés). Dans le rapport 2020 susmentionné, voici dans l'ordre les dix premières cyberpuissances mondiales : les États-Unis, la Chine, la Grande Bretagne, la Russie, la Hollande, la France, l'Allemagne, le Canada, le Japon, et l'Australie.

Ces trois études renseignent de la complexité à évaluer en toute objectivité ce qu'on pourrait considérer comme une cyberpuissance, étant entendu que le concept est lui-même tout récent, et donc en pleine construction. Pour l'instant, il ne saurait ainsi avoir une seule et unique façon de le définir et de l'envisager. On aurait par exemple pu mobiliser une autre étude telle que la National Cyber Security Index (qui s'articule autour du niveau de développement numérique dans un pays et son indice de cybersécurité nationale), ou encore d'autres facteurs tels que le classement mondial des meilleures universités en matière de cybersécurité, la performance de certains pays dans les tournois internationaux de hackers éthiques, etc. Mais jusque-là cela n'aurait pas suffi à trancher la question sur qui est une cyberpuissance et qui ne l'est pas. Les notions même de cyberespace et de puissance faisant l'objet de représentation selon différents paradigmes, il n'est pas surprenant que ces différences rejaillissent sur la perception que nous pouvons avoir de ce qu'est une cyberpuissance.

III.4. Tentative d'énonciation des critères d'une cyberpuissance

Dans le cadre de cette analyse, je vais vous proposer une liste de critères de cyberpuissance qui [au regard de ce qui a été dit précédemment] sera certainement non exhaustive donc incomplète, probablement discutable. Elle est à la fois inspirée de différentes études comme celles que nous avons évoquées, et des travaux de chercheurs (Olivier Kempf, Bertrand BOYER, etc.). Certains éléments reviennent, même si reformulés avec quelques nuances sur la forme. Pour être considéré comme une cyberpuissance en 2020, un pays devrait remplir les six principaux critères suivants :

- Avoir un niveau élevé de numérisation (maturité cyber) de la société : ceci peut être mesuré à partir d'un ensemble de facteurs tels que le taux de connectivité et de pénétration d'internet, d'usage d'équipements numériques (ordinateur personnel, Smartphone, tablette, etc.), le niveau de développement des infrastructures, la part de l'économie numérique dans le PIB du pays, etc.
- L'existence d'un écosystème d'entreprises conférant une certaine autonomie industrielle et technologique en matière de numérique (fabrication du matériel informatique et de télécommunication, conception et développement des logiciels, bref, maîtrise de la chaîne de valeurs du digital).

- L'existence d'une pensée et d'une vision stratégique relative au cyberespace, ainsi que d'une doctrine en la matière. Cette doctrine doit déterminer la posture stratégique [identifiable] guidant les actions du pays dans le cyberespace, aussi bien sur le plan interne qu'externe.
- L'existence d'un écosystème de formation (universités, grandes écoles) et de recherche et développement performant, capable d'alimenter l'innovation industrielle et supporter le besoin du marché en expertise.
- L'existence d'un dispositif cohérent de cybersécurité et de cyberdéfense (disponibilité des ressources humaines et financières à la hauteur de la vision, des moyens techniques et opérationnels, juridiques et organisationnels, etc.), avec une capacité effective de LIO (Lutte Informatique Offensive) et LOD (Lutte Informatique défensive).
- L'existence d'une cyberdiplomatie active et perceptible : elle peut se manifester par une représentation marquée dans les instances internationales de gouvernance du cyberespace (établissement des normes, modification du droit international pour le cyberespace, groupe d'expert technique, etc.). Il s'agit aussi de développer des réseaux de partage d'information, ainsi que la capacité à entretenir des rapports de coopération ou des alliances avec les autres Etats, en les calibrant sur leur niveau de puissance (plus fort, plus faible ou relativement égal).

Un nombre important d'utilisateurs, la capacité à coopérer et à influencer la production des normes, la capacité de recherche et d'innovation, une base industrielle et technologique, des infrastructures développées, le capital humain (la qualité de la formation et le vivier des experts), la volonté assumée d'utiliser les moyens cybers pour des objectifs stratégiques nationaux : voilà quelques critères pouvant faire d'un pays une cyberpuissance, en tout cas selon la conception actuelle de cette notion. En admettant ce référentiel, quelles seraient donc les principales cyberpuissances dans le monde aujourd'hui ?

IV. Quelles sont les cyberpuissances actuelles ?

Malgré les disparités dans les critères de mesure d'un indice à l'autre, ainsi que certaines nuances dans les analyses des spécialistes, un consensus se dégage sur les capacités cyber, avancées d'au moins trois pays : les États-Unis, la Chine, et la Russie. Au demeurant, s'inscrivant dans la continuité des rapports historiques et géopolitiques qui les lient, ces pays ont très tôt rendu public leur document de cyberstratégie nationale (et de doctrine) affichant aux yeux du monde les ambitions et la volonté de puissance dans le cyberespace qui animent chacun d'eux. Sur la base des critères que nous venons de définir, on peut aisément reconnaître le niveau plutôt avancé (et suffisamment documenté) de ces pays, particulièrement des trois premiers. En termes de maturité cyber, d'autonomie stratégique sur les solutions, d'écosystème d'experts au service de l'Etat, d'influence sur la gouvernance mondiale d'Internet etc., ils sont parmi les leaders. Ces pays font partie de ce que le général O. Kempf appelle la « ligue des champions » des puissances cyber !

Ce qui de mon point de vue fait assurément de ces pays des cyberpuissances, c'est l'aptitude à avoir réalisé une démonstration de puissance efficace au moins une fois aux yeux du monde : par l'utilisation des moyens numériques, ils ont montré leur capacité à influencer des situations géopolitiques dans d'autres pays. Ainsi, on connaît bien l'affaire de l'ingérence russe dans les élections américaines de 2016, de l'opération *Olymppic games* (Stuxnet) des américains en Iran, ou encore des multiples opérations chinoises contre les entreprises occidentales (Shady Rat, Titan Rain, etc.) pour ne citer que ces quelques exemples. En matière de capacité cyber, Etats-Unis, Chine, Russie jouent en ligue des champions. Appelons les *cyberpuissance de catégorie 1*, car elles sont capables d'exercer leur volonté propre et d'influencer celle des autres (pays comparables en niveau) dans le cyberespace.

À leur suite et toujours en s'appuyant rigoureusement sur nos critères, on peut ajouter la Grande Bretagne, la France, l'Inde, l'Australie, le Canada, (et probablement d'autres) comme des cyberpuissances « relatives ». De mon point de vue, ils font partie des pays capables d'exercer leur volonté de façon autonome dans le cyberespace et donc de résister [voir se défendre] contre les agressions extérieures. La limite étant leur capacité à influencer la volonté des autres pays de niveau comparable, notamment des cyberpuissances de catégorie 1. D'où la notion de relativité introduite ici, permettant de les classifier comme *cyberpuissance de catégorie 2*.

IV.1. L'état d'Israël, un cas particulier

Le cas de l'État d'Israël me semble être intéressant à regarder de près, au regard de sa stratégie un peu particulière. Partant d'une situation historique, géographique et culturelle tout à fait singulière, ce pays a su se construire un positionnement de cyberpuissance pour le moins curieux. En effet, c'est au début des années 2010 qu'à la demande du premier ministre israélien Benjamin Netanyahu, l'ancien général Isaac Ben-Israël a posé les bases d'une stratégie de puissance dans le cyberespace pour son pays. En tant que conseiller spécial du premier ministre en la matière, il a créé le Bureau National du Cyber (*National Cyber Bureau*[1]) et lancé l'Initiative Nationale du Cyber en 2010, dont plusieurs spécialistes s'accordent à dire que c'est la fondation de la cyberpuissance de l'Etat d'Israël telle qu'on la connaît aujourd'hui.

L'un des atouts majeurs de cette démarche, c'est son ancrage conceptuel dans l'expérience historique et l'imaginaire symbolique. En effet, les dirigeants israéliens ont commencé par questionner l'étymologie même de la notion de « cyber » dont l'origine est attribuée au grec (même si c'est un fait que nous contestons dans notre propre démarche). La notion de cyber a donc été redéfini par le concept « sb'r » qui pour eux renvoi au domaine de la pensée, de l'intelligence, de la conceptualisation. Comme autre atout, ce pays peut aussi compter sur le fort sentiment d'appartenance qu'à sa population à la nation, et à une société fortement militarisée (service militaire obligatoire). Ce qui leur permet aujourd'hui d'avoir une structure organisationnelle du domaine cyber très militaro-centré, mais avec un fonctionnement collaboratif voir organique avec les autres composantes de la société (universités, startups, etc.).

Au-delà de ces aspects culturels et organisationnels, cette stratégie israélienne, basée sur la théorie du « cygne noir[2] », s'articule autour de deux axes majeurs. Le premier c'est le développement d'un écosystème intégré de cybersécurité et cyberdéfense (plutôt que d'un géant mondial du numérique) tel que le fameux *CyberPark*. Initié depuis 2014 par le gouvernement israélien, il s'agit d'un pôle d'innovation cyber constitué de startups, de centres de recherches (privés et publiques), d'industriels locaux et étrangers, de structures universitaires et militaires, tous réunis dans une même zone géographique (Beer Sheva).

Le second axe de la stratégie est le pari sur la compétence et le talent d'une ressource humaine locale, et leur capacité d'innovation. L'esprit d'initiative et d'entreprenariat est fortement encouragé, avec des résultats remarquables à la clé. Ainsi, avec environ 436 entreprises cyber et un chiffre d'affaires global de $6,5 milliards à l'export (en 2020), Israël est le deuxième exportateur de solution cyber après les

[1] Devenu aujourd'hui l'INCD (*Israel National Cyber Directorate*).

[2] La théorie du cygne noir est un concept développé par Nassim Nicholas Taleb dans son ouvrage intitule *Le cygne noir*. En gros, cela consiste à se préparer et à prévoir l'imprévisible.

Etats-Unis, notamment dans le domaine stratégique (couvrant ainsi 5% du marché mondial). De même, 20% d'investissement mondial en cybersécurité est fait en Israël. Là encore, c'est le second rang directement derrière les USA.

L'ensemble de ces éléments ont permis de bâtir une cyber-résilience comme facteur de puissance, par la création des interdépendances stratégiques avec les cyberpuissances de catégorie 1, en particulier les Etats-Unis. Les entreprises et investisseurs américains sont notamment très présents dans l'écosystème israélien (plusieurs solutions du marché sont d'ailleurs coproduites par les entreprises des deux pays). Dans ce contexte, beaucoup considèrent Israël comme deuxième puissance cyber du monde, directement derrière les USA.

Mais la trop forte présence américaine dans son écosystème est au point où certains spécialistes se posent la question d'une hyper-dépendance, et de la capacité réelle d'autonomie cyber d'Israël sans ce parapluie. Sans l'apport du pays de l'oncle Sam et sur la base de l'ensemble des critères largement explorés *supra*, dans quelle catégorie se retrouverai l'Etat d'Israël ? En gros, ce pays peut-il exercer sa volonté et influencer celle des autres dans le cyberespace sans l'aide des États-Unis ? C'est une question difficile à trancher [même si je penche pour la *catégorie 2*] ! D'où la particularité de ce modèle que le reste du monde observe avec intérêt. A défaut de le reproduire, ce modèle peut-il inspirer l'Afrique dans une démarche de cyberpuissance ?

IV.2. Emergence d'une nouvelle forme de puissance

Pour récapituler, on peut distinguer des cyberpuissances de catégorie 1 (pays ayant la capacité d'exercer leur propre volonté et d'influencer celle d'autres pays de niveau comparable dans le cyberespace), et des cyberpuissances de catégorie 2 (pays capables d'exercer leur volonté de façon autonome, mais pas d'influencer celle des autres). Ces capacités sont en cohérence avec le niveau de maturité quant aux critères que nous avons évoqués (plus un pays sera avancé sur l'ensemble des critères – et en aura fait la démonstration -, plus il se rapprochera du statut de cyberpuissance de catégorie 1). Tous les autres pays (notamment la plupart des pays africains) dépendent des technologies, normes, connaissances, informations produites ailleurs. Ce qui les rend perméables à l'influence extérieure et incapable de se défendre convenablement. Bien évidemment, cette posture les éloigne du statut de puissance cyber.

J'aimerai convoquer ici une troisième catégorie de cyberpuissance, qui relève de la nature même du cyberespace et de son caractère hybride. Cette nature singulière amène les auteurs de l'article "*Qu'est-ce-qu'une cyber-puissance ?*" à postuler que la *théorie westphalienne*, qui fait des Etats les principaux acteurs des relations internationales, n'est pas applicable au cyberespace ! Selon ces chercheurs membres de l'Institut *Open Diplomacy* :

> La grille de lecture westphalienne du cyberespace est totalement incomplète car elle omet des acteurs absolument déterminants dans les rapports de force : les acteurs privés. À l'instar des BATX (Baidu, Alibaba, Tencent et Xiaomi) et des GAFA (Google, Apple, Facebook et Amazon), il y a des acteurs dont la puissance capacitaire et normative rivalise avec la puissance publique et détermine le cours du cyberespace. Il ne s'agit pas que de prestataires de services qui rendraient service aux acteurs westphaliens - les États - et en deviendraient une extension. Il s'agit d'acteurs qui s'autonomisent dans le champ de force. Des producteurs de hardware - le fabricant de puces électroniques comme le producteur de terres rares - aux créateurs de software - le développeur de logiciels comme l'inventeur d'un OS - ils sont des acteurs à part entière de la puissance cyber, parfois autonome des frontières géopolitiques classiques[3].

[3] Adrien Vanheste, Jean-Baptiste Boyssou et Thomas Friang, "*Qu'est-ce-qu'une cyber-puissance ?*", Open Diplomacy, 2020.

Ainsi, certains acteurs à priori privé (GAFAM, BATX, etc.) qui par leur modèle économique (captation et valorisation de l'information) et leur puissance financière ont la capacité d'influencer la volonté de certains Etats dans le cyberespace, peuvent donc aussi être considérer comme des cyberpuissances d'une autre catégorie, en dehors des champs classiques de la puissance. Il faut noter qu'en réalité, c'est aussi grâce à la performance de ces multinationales et à leur collaboration désormais démontrée avec les services de renseignement étatiques que les pays de la première catégorie ont construit leur puissance numérique. Aux Etats-Unis par exemple, on parle déjà de complexe militaro-internet et industrialo-internet pour tenter de décrire la relation organique qui lie ces géants à leur État. On peut en dire autant en Russie, en Chine, en Israël.

Dans le même temps, les très célèbres et tous puissants dirigeants de ces oligopoles américains du numérique ne font aucun mystère de leur volonté de constituer une puissance propre et distincte de leur État, volonté qu'ils manifestent en parole et en action. Ce qui place ces acteurs dans un positionnement dual et particulier dont il appartient aux géo-politologues d'en explorer les contours. Eric Emerson Schmidt, ancien PDG de Google, l'avait clairement exprimé dans en ces termes : « *les États sont inefficients, nous sommes efficaces, nous avons vocation à les remplacer…* ». L'ambition ne saurait être plus limpide !

Entre temps, Elon Musk (fondateur de l'entreprise à succès Tesla) avec son projet SpaceX s'est lancé dans des missions d'exploration de l'espace extra-atmosphérique (la Lune, la planète Mars, etc.), avec pour ambition de déployer des milliers de satellites de communication ainsi que d'y créer les conditions de la vie pour l'homme. Il dispose pour ce faire des ressources financières que beaucoup de pays ne peuvent pas se permettre, et que même la toute puissante et historique NASA n'est plus en capacité de mettre pour le suivre. On pourrait aussi parler de Facebook avec sa tentative récente de création d'une monnaie (le *Libra*), ou de Bill Gates qui est un des principaux donateurs de l'OMS. Tous s'attaquent à des fonctions dites régaliennes, qui étaient jadis le domaine réservé des Etats (au sens Westphalien).

Ainsi, leur présence massive dans les instances de gouvernance d'Internet, leur capacité à produire des normes et à faire du lobbying auprès des Etats pour peser sur les lois régulant leur secteur d'activité, leur propension à construire des infrastructures (data centres, câbles fibres optiques sous-marin, etc.) et des centres de recherche à travers le monde, leur volonté de remodeler les systèmes éducatifs, de s'immiscer dans les processus démocratique, d'influencer les habitudes de consommation et les comportement sociaux, de financer des écosystèmes entiers et bien d'autres leviers encore par lesquels ils peuvent se « substituer aux états », confèrent un pouvoir certain et concret à ces acteurs.

Tant et si bien que les concepts de « colonisation numérique », « cyber-colonisation » ou encore « cyber-impérialisme » ont émergé et font l'objet de plus en plus de publications. Loup Ducol le démontre à suffisance dans cet article paru en 2019. Le géographe américain Joel Kotkin parle lui de *L'Avènement du néo-féodalisme* [titre de son livre] pour décrire une nouvelle oligarchie du numérique qui souhaite dominer et modeler le monde de demain grâce à la technologie !

Plus puissant que beaucoup d'Etats dans le monde, certains pays n'hésitent plus à considérer officiellement les géants technologiques comme tel. C'est notamment le cas du Danemark ! En 2017, la ministre danoise des affaires étrangères a annoncé la création d'un poste d'ambassadeur du numérique pour représenter leurs intérêts auprès de ces géants de l'innovation technologique, notamment ceux de la Silicon Valley. Anders Samuelsen, qui dans cette annonce a fait la même analyse que je viens de vous présenter, résume bien la situation dans la phrase suivante : « *Ces firmes sont devenues un nouveau*

type de nation et nous avons besoin de nous confronter à cela. ». Le mot est lâché ! Plus que des nations, ce sont des organisations que les spécialistes de géopolitique qualifieraient de supranationales, qui remplissent bien les critères de cyberpuissance, et que nous inscrivons donc dans une *catégorie 3* (acteur non étatique capable d'influencer la volonté de d'autres acteurs dans le cyberespace, y compris celle des Etats). En allant au bout de cette logique, on peut d'ailleurs tout à fait se risquer ici à considérer ces acteurs comme des *smart power* (car ils sont capables à la fois de contraindre et d'influencer !).

Bien entendu il s'agit d'une classification forcément partielle, incomplète et donc à parfaire, ne servant ici qu'à soutenir un raisonnement.

V. L'Afrique : future cyberpuissance

Avec le recul, les spécialistes s'accordent à dire que les technologies et protocoles qui ont permis la construction initiale du réseau internet avaient été conçus et développés dans un esprit libertaire, une volonté d'ouverture, de partage, etc., mais sans intégrer dans ses fondements les objectifs de sécurité puisque la question ne se posait pas à l'époque. Le réseau a évolué très rapidement et dans ce même état d'esprit, en ajoutant des briques à l'architecture initiale "non sécurisée" (qui constitue le cœur, la dorsale de l'internet actuel) et en s'étendant progressivement à travers le monde. Cette évolution du réseau s'est poursuivie dans les mêmes conditions jusqu'à vers la fin des années 1980, à l'apparition des premiers virus informatiques...

Face au développement de la cybercriminalité et à la nécessité grandissante de sécurisation des réseaux, plusieurs technologies et solutions sortent des laboratoires tous les jours. Le problème est qu'elles viennent juste se greffer ou s'agréger autour du cœur initial du réseau et ses protocoles sources (TCP/IP) qui, on l'a dit, sont "non sécurisés" par nature. D'après le Français *Louis POUZIN* (l'un des pères fondateurs d'internet, celui qui a inventé le "*datagramme*"), pour sécuriser efficacement le réseau internet il faut casser toute l'infrastructure actuelle (surtout l'architecture initiale) et le reconstruire de zéro. Car à l'époque, dit-il, "*la sécurité n'était pas du tout leur sujet*". Ce que confirme *Bernard Barbier*, qui a travaillé au cœur des problématiques de souveraineté numérique et de cyberespionnage en tant qu'ancien directeur technique du renseignement extérieur (DGSE) français. Le 12 juillet 2010 dans le journal l'Usine nouvelle, il déclare que « *Internet n'a pas été conçu pour être sécurisé* ». Cela a le mérite d'être clair !

Dans ce schéma global, les pays africains sont ceux ayant le plus de déficit sur tous les critères évoqués ci-dessus. L'Afrique demeure aujourd'hui le continent le plus en retard dans sa transformation numérique, car le moins nanti en matière d'infrastructures des technologies de l'information et de la communication. On parle d'un taux de pénétration de 39% en Mars 2020, avec environ 523 millions d'africains connectés[4]. Examinons maintenant de près une hypothétique ambition de puissance numérique africaine sur la base d'une analyse SWOT (Forces, Faiblesses, Opportunités et Menaces).

V.1. Les atouts (Forces) de l'Afrique pour devenir une cyberpuissance

Le faible niveau de "cybérisation" du continent que nous venons d'évoquer peut s'avérer être une aubaine si bien exploitée par les stratèges africains, au regard du potentiel d'environ 1 milliard de personnes à connecter dans les 20 prochaines années. Ainsi, au lieu de continuer le déploiement de nos infrastructures en adoptant, on vient de le voir, un modèle exogène initialement conçu sans aucune

[4] Source : *World Internet Users Statistics*

préoccupation de sécurité et dans un cadre épistémique qui n'est pas le nôtre, nous avons la possibilité de bâtir une nouvelle génération d'infrastructures sur la base d'un modèle endogène d'innovation (Cf modèle MAIT). Cela nous permettra de privilégier le développement et l'usage des technologies et solutions ayant la sécurité embarquée, donc consubstantielle à leurs conceptions. Puisque nous partirons de plus loin que toutes les grandes puissances actuelles, nous aurons à l'arrivée un cyberespace plus sûr et plus protégé.

En plus de notre retard [en infrastructure] qui peut tourner en avantage si nous manœuvrons bien, la population jeune et le potentiel de croissance démographique en Afrique est une autre force considérable. En effet, en passe de devenir le plus grand marché unique du monde (suite à la mise en place de la Zone de Libre Échange Continentale prévu sur 52 pays) et avec une population estimée par les nations unis à 2,5 milliards d'ici 2050, l'Afrique a pour elle sa démographie comme facteur de puissance. De plus, la structure de cette population [essentiellement jeune et friande des solutions numériques] est propice à la construction d'une cyberpuissance, étant donné aussi la sensibilité de l'univers du cyberespace aux capacités d'innovation, de créativité et de création exponentielle de la valeur par l'effet réseau (loi de Metcalfe).

En matière d'innovation justement et de capital humain qualifié, le continent africain regorge d'un important vivier d'experts dans ses diasporas qui peuvent être mobilisés au service d'une vision claire et porteuse d'espoir. Tout cela n'est possible que sous réserve d'une stratégie ambitieuse et cohérente de transformation numérique, qui s'appuie sur un modèle d'innovation technologique propre à l'Afrique. Les expériences chinoise et indienne peuvent nous renseigner, aussi bien sur ce facteur démographique que sur la nécessité d'une approche endogène comme vecteur de puissance dans le cyberespace.

L'autre atout majeur du continent africain dans la perspective d'une ambition de cyberpuissance est son immense richesse en matières premières et ressources naturelles. Nous l'avons vu, l'un des critères constants pour devenir une puissance cyber est l'existence d'une base industrielle et technologique. Or les fondements de toute industrie c'est la matière première, et l'énergie. En l'occurrence, l'Afrique regorge de gisements de terres rares utiles à l'industrie numérique, lesquelles font d'ailleurs l'objet de prédation par les puissances actuelles qui souhaitent maintenir leur position.

La question énergétique est similaire : plusieurs analyses géopolitiques attribuent l'instabilité récurrente de certains pays à l'ingérence des puissances étrangères qui se battent pour le contrôle des sources d'énergie sur le continent (uranium au Niger, pétrole dans plusieurs autres pays, etc). Pour être en mesure de construire une base industrielle solide qui prend en compte toute la chaîne de valeur de d'une économie numérique, les dirigeants africains devront donc reprendre la maîtrise de nos matières premières et ressources naturelles. C'est un objectif certainement pas simple, mais capital ! D'où là encore, la nécessité d'une volonté ferme et d'une stratégie cohérente à l'échelle continentale, et qui s'inscrit dans la durée.

V.2. Les défis et contraintes (Faiblesses) que l'Afrique doit affronter

- La nécessité d'être uni et d'agir à l'échelle du continent ! Divisée, l'Afrique ne pourra prétendre à devenir une cyberpuissance. De même, aucun pays africain tout seul ne pourra faire face à toutes les contraintes (humaines, économiques, etc.) pour réaliser cet objectif. L'Afrique en tant que continent doit donc clairement afficher sa volonté et son ambition de devenir une cyberpuissance à un certain horizon, et prendre toutes les dispositions qui s'imposent pour y

parvenir. Malgré tous nos atouts, rien de tout ceci n'est perceptible aujourd'hui, même pas dans l'Agenda 2063 de l'union africaine !

- La nécessité d'élaborer une pensée stratégique du cyberespace propre à l'Afrique, et d'en dégager une cyberstratégie cohérente permettant progressivement de prendre toutes les mesures pour remplir les critères d'une cyberpuissance.
- L'urgence d'élaborer et de mettre en place un plan africain d'industrialisation numérique, sur la base d'un modèle d'innovation technologique qui nous est propre (MAIT). Ce modèle, qui prône la conception des solutions à partir des référentiels endogènes, va nous permettre de dépasser la logique actuelle considérant le numérique comme outil d'accélération du développement socio-économique et d'expression démocratique (paradigme exogène), pour l'inscrire dans une perspective de renaissance kamit.
- Le manque d'une main d'œuvre qualifiée, et l'existence d'un capital humain supposément expert mais dont le niveau de formation est soit discutable, soit inadapté. Ce qui pose le problème de l'orientation de la formation (elle est au service de quelle ambition ?), ainsi que de sa qualité et son niveau d'exigence. Ce déficit peut en parti être pallié par la mobilisation des nombreux experts de la diaspora, et par l'élaboration d'un nouveau standard de formation pour la population jeune et dynamique présente sur le continent.
- La trop faible présence des représentants officiels de l'Afrique dans les instances techniques et de gouvernance d'internet, capables de défendre les intérêts du continent dans le cyberespace. Conséquences, nous subissons toutes les normes technologiques décidées à partir de ces instances (bien souvent sans nous et parfois contre nos intérêts), nous négocions des partenariats presque toujours en position de faiblesse, nous avons une cyber-diplomatie inexistante du fait qu'il n'existe pas de position africaine sur les grandes questions du cyberespace (évolution et adaptation du droit international dans le cyberespace, régulation des cyberarmes, cadre de réponse en cas d'une cyber-agression étatique établie , etc.).

V.3. La concomitance d'éléments positifs (Opportunités) propice à cette démarche en Afrique

Une population jeune et dynamique ; foisonnement d'initiatives innovantes dans la jeunesse et l'émergence d'un écosystème de startups ; l'attractivité montante du continent africain pour les investissements extérieurs dans les projets numériques ; la multipolarité actuelle du monde, et les rapports de force entre puissances dont l'Afrique est la convoitise ; la vulgarisation des idées du panafricanisme, de l'Afrocentricité et de la renaissance africaine qui font de plus en plus naître chez les jeunes la prise de conscience d'une expérience historique commune, d'un destin et des dessins communs en tant que africains; richesse en matières premières et sources d'énergie ; mais surtout, la prise de conscience des dirigeants africains qui ont pour la plupart décider de s'appuyer sur la transformation numérique pour accélérer le développement socio-économique de leur pays et améliorer le niveau de vie de leurs citoyens. Cette prise de conscience se traduit par exemple par l'initiative Smart Africa, dont la vision est de « transformer l'Afrique en un marché numérique unique » à l'horizon 2030 !

Tous ces éléments mis ensemble positionne l'Afrique dans une fenêtre historique et peut être unique pouvant lui permettre d'entreprendre une stratégie de cyberpuissance ! C'est une opportunité à saisir, mais qui nécessite un pivot stratégique vers un nouvel horizon.

V.4. Menaces potentielles sur une démarche africaine de cyberpuissance

L'Afrique a toujours été la convoitise des puissances étrangères, aussi bien pour ses ressources naturelles que humaines. Depuis quelques années, on observe une montée en puissance sur le continent

d'acteurs qui deviennent de plus en plus influents (Chine, Russie, Turquie), contestant ainsi les positions dominantes d'acteurs dit historiques tels que la France, les États-Unis, l'Angleterre, etc. Si ces nouveaux rapports de force peuvent constituer une marge de manœuvre stratégique pour les africains, il faut bien souligner que chaque acteur est présent pour ses intérêts ! Lesquels peuvent être en contradiction avec une ambition de puissance que porterai l'Afrique.

Certaines de ces puissances étant dépendantes des matières premières et des sources d'énergies exploitées dans nos pays pour maintenir leur positionnement, elles ne cesseront jamais de travailler à la division, à l'affaiblissement et à l'instabilité du continent, empêchant ainsi toute initiative d'industrialisation. A mon avis, il s'agit de la menace majeure dans notre contexte, que l'économiste Dr. Howard Nicholas décrit brillamment dans ses analyses les raisons profondes du sous-développement de l'Afrique subsaharienne.

La seconde menace, qui bien souvent découle de la première, c'est l'ensemble des instabilités politiques (crises postélectorales, etc.), économiques (corruption, plans d'ajustements, etc.) et sécuritaires (rebellions militaires, terrorisme, etc.) que l'on observe dans plusieurs pays africains. Associé à ce que les ONG appellent la mauvaise gouvernance, l'ensemble de ces facteurs qui fragilisent le continent ne lui permettent pas d'exploiter ses atouts et de surmonter ses contraintes. Ce qui constitue un frein réel à une ambition de cyberpuissance, et même de puissance tout courte.

Conclusion

Au regard de la nature complexe et transverse du cyberespace, la notion de puissance a elle aussi évolué pour s'y adapter. Cette nouvelle forme d'expression de la volonté, la cyberpuissance, dépasse le cadre classique des Etats et voit émerger de nouveaux acteurs privés : les géants du numérique. Chacun de ces acteurs [pays et entreprises listés *supra*] reconnu aujourd'hui comme cyberpuissance exercent sa volonté dans l'espace cybernétique à des niveaux différents, que nous avons classé en trois catégories. La dualité des entreprises technologiques qui à la fois constituent l'un des moyens de la cyberpuissance de leurs Etats et manifestent une volonté de puissance propre, est un phénomène nouveau qu'il convient de creuser. Dans le cas de l'Afrique, devenir une cyberpuissance reviendrait à trouver une cohérence d'ensemble, un équilibre entre cybersécurité, cyberdéfense et cyberstratégie, nous permettant d'avoir au minimum une capacité d'action autonome et souveraine dans le cyberespace (catégorie 2) à l'échelle continentale. Le but n'est pas d'influencer quiconque, mais d'être maître de notre volonté, de décider et d'agir librement selon nos propres choix et pour nos propres intérêts dans le cyberespace. C'est possible ! Car l'Afrique dispose en son sein d'un riche héritage historique et culturel en matière de puissance, et de suffisamment d'atouts contemporains nécessaires pour y parvenir. Même les contraintes que nous avons évoquées ne sont pas insurmontables. Mais je le répète, tout réside dans l'ambition des acteurs, leur volonté d'agir, et une pensée stratégique autoréférentielle.

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, « L'Afrique peut devenir une cyberpuissance », Note N° 12 — LARC, Mars 2024.