Laboratoire Africain de
Recherches en Cyberstratégie

Route de la soie numérique et affrontements Chine-USA : les enjeux pour l'Afrique

Par DJIMGOU NGAMENI

Avril 2021

Résumé :

Depuis quelques années maintenant, le monde entier assiste à un affrontement entre deux puissances qui ont théorisé leur domination du monde par les technologiques numériques et le cyberespace. Cette rivalité trouve aujourd'hui son point culminant sur la technologie sans fil de cinquième génération (5G), dont chaque partie est convaincue que sa maîtrise lui donnera une position dominante dans les prochaines décennies. D'où le recours au cyberespionnage de part et d'autre, avec pour finalité de garder l'avance sur son vis-à-vis. Impacté par cet affrontement (notamment à travers le projet chinois de route de la soie numérique qui débouche en Afrique), il revient aux pays du continent d'élaborer une stratégie endogène et de développer leurs propres capacités de cyberdéfense pour y faire face.

Introduction

La « nouvelle route de la soie », rebaptisé « initiative ceinture et route » (en anglais *Belt and Road Initiative*, avec l'acronyme **BRI**) est l'un des programmes les plus ambitieux du président chinois *Xi Jinping*. Prévue pour projeter l'influence géopolitique transformatrice de la Chine à travers le monde, l'ampleur et la portée du projet sont sans précédent. Beijing a consenti 4 000 milliards de dollars d'investissements dans des projets d'infrastructures et de développement dans 65 pays, touchant 70% de la population mondiale et 75% des réserves d'énergie du monde. Le programme est conçu pour relier les principaux centres économiques de l'Eurasie par voie terrestre et maritime, dont beaucoup servaient autrefois à l'ancienne route de la soie il y a deux mille ans.

Selon le magazine d'information *The Diplomat*, « la BRI a pour objectif de stabiliser les périphéries occidentales de la Chine, de relancer son économie, de propulser des institutions économiques internationales non occidentales, de gagner de l'influence dans d'autres pays et de diversifier les fournisseurs / itinéraires commerciaux tout en contournant le pivot américain vers l'Asie ». Après avoir pris le temps de fabriquer des géants économiques (notamment les BATX dans le domaine numérique), l'empire du milieu par cette initiative les emmènent à la conquête de nouveaux marchés avec dans leurs bagages à la fois le financement et les technologies (5G, câbles sous-marins, système de navigation par satellite, etc.). Nous sommes donc face à une démonstration de la puissance.

Pour pouvoir réaliser cette ambition en gardant une avance sur ses rivaux (principale les Etats-Unis), la Chine mobilise tous les moyens et outils à sa disposition. Dans un rapport adressé à ses clients, l'entreprise *FireEye*[1] fait état de preuves d'une augmentation des opérations de cyberespionnage liées à la BRI. Ce rapport indique notamment que « *L'activité de cyberespionnage liée à l'initiative comprendra probablement l'émergence de nouveaux groupes et acteurs des États-nations. Compte tenu de l'éventail des intérêts géopolitiques touchés par cette entreprise, il peut être un moteur pour les cyber-acteurs des États-nations émergents d'utiliser leurs capacités* ».

[1] *FireEye* est une entreprise américaine de cybersécurité, bien connue sur le marché. Plusieurs de ses clients sont des organisations publiques américaines.

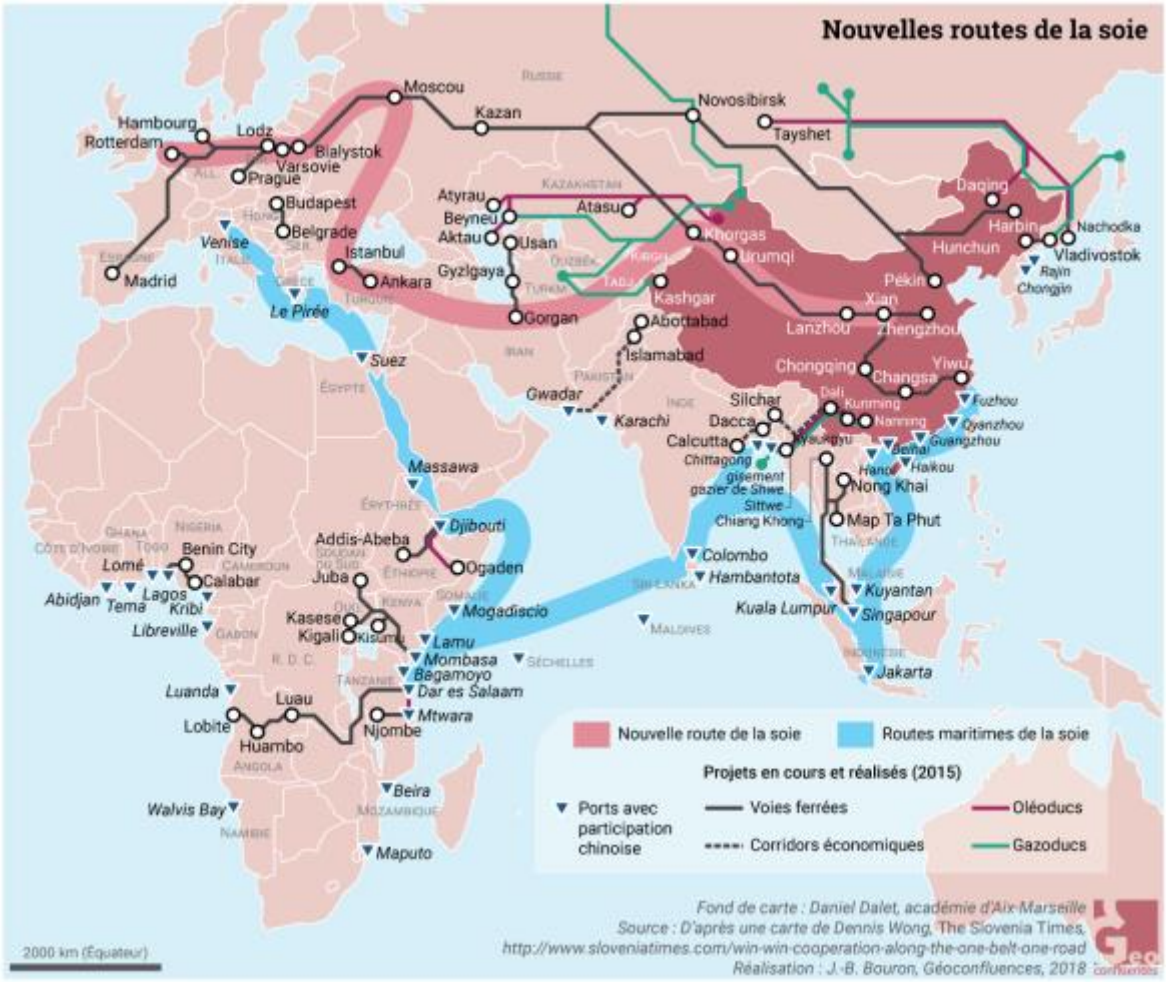

Image 1 : Nouvelles routes de la soie

La BRI vise également à renforcer l'influence géopolitique et économique de la Chine en Afrique, en capitalisant sur les investissements importants dans les infrastructures réalisées sur le continent. Le Kenya en particulier a fait l'objet d'une attention accrue en raison de sa situation géographique stratégique, notamment pour la composante maritime de cette nouvelle route de la soie chinoise (connue sous l'appellation China's Maritime Silk Road Initiative – MSRI).

Au début de l'année 2018, le Kenya a annoncé qu'il ferait du lobbying pour des projets régionaux dans le cadre de la nouvelle route de la soie. C'est d'ailleurs dans cette optique que la Chine a ainsi financé la construction d'un chemin de fer à écartement standard de 480 km entre la ville portuaire kényane de Mombasa et sa capitale Nairobi. D'après le plan, ce chemin de fer devrait éventuellement s'étendre aux pays voisins tels que l'Ouganda, le Rwanda et le Burundi afin de les relier au port de Mombasa. Cependant, en mai 2018, le Kenya a annoncé qu'il ne signerait pas l'accord de libre-échange en cours de discussion entre la Chine et les États de la Communauté de l'Afrique de l'Est (EAC), ce qui aurait entraîné des tensions entre Beijing et Nairobi.

La route de la soie numérique en action !

C'est dans ce contexte qu'entre en jeu, au-delà des aspects publics du projet BRI (tels que les infrastructures routières, chemins de fer, voies maritimes), un autre volet plus subtil mais tout aussi important dans le dispositif global de ce programme d'envergure : il s'agit de la "***Digital Silk Road***" ! En effet, le plan directeur du projet BRI rendu public en 2015 évoque la création « *d'une route de la soie de l'information* » comme un des piliers majeurs pour la réussite de cette aventure. L'idée est de s'appuyer sur les géants industriels chinois pour améliorer la connectivité numérique tout au long de la route (et même au-delà) par la mise en place des infrastructures de télécommunication telles que l'installation des câbles à fibre optique transcontinentaux (on peut par exemple citer le cas de *Huawei Marine Networks Co*, qui a posé un câble de 6 000 kilomètres entre le Brésil et le Cameroun), la construction des centres de données (*data centers*) et des villes intelligentes (*smart cities*), le développement des services en ligne, etc.

L'ambition de puissance et d'influence qui caractérise cette initiative repose donc aussi sur l'outil cyber, et elle (cette ambition) reste intacte même dans le cyberespace. Le président *Xi Jinping* l'a d'ailleurs réaffirmé en 2017 lors du tout premier forum sur le projet BRI à Beijing, en insistant sur la nécessité d'accélérer l'intégration des technologies innovantes dans son implémentation.

C'est donc sans surprise que dans le *rapport CTA-2018-0816*[2] de l'entreprise Américaine *Recorded Future*, le volet technique nous révèle quelques détails intrigants. Au début du mois de juin 2018, leur centre d'analyse cybernétique a observé *l'adresse IP 166.111.8.246* balayant de manière agressive les ports [de communication] 22 (SSH), 53 (DNS), 80 (http), etc. [en destinations] de différents fournisseurs Internet, hébergeurs et opérateurs de télécommunications kényanes. Les analystes ont aussi observé que des plages [d'adresse internet] dédiées à l'autorité portuaire kényane (*Kenya Ports Authority)*, une société d'État chargée de l'entretien et l'exploitation de tous les ports du Kenya.

Au-delà du charabia technique, ces éléments schématisent bien la phase de reconnaissance (ou d'identification des failles) dans une cyberattaque organisée. *Recorded Future* a également identifié des activités de reconnaissance de réseau dirigées vers le bureau des Nations Unies à Nairobi, l'Université *Strathmore* du Kenya et plus largement dans le réseau de l'éducation nationale. L'adresse *IP 166.111.8.246* de l'attaquant a été retracé et a permis de remonter jusqu'à la Chine, précisément à l'Université *Tsinghua*. A la lumière de ces indices, il apparait distinctement que le Kenya a été la cible d'une opération de cyberespionnage en provenance de la Chine.

[2] Étude intéressante intitulée "Route de la soie numérique" et menée par des étudiants de l'Ecole de Guerre Économique, portant sur le projet *Digital Silk Road* de la Chine.

Rôle trouble des universités chinoises dans les opérations de cyberespionnage

L'Université *Tsinghua* est une institution publique située dans le district de *Haidian* à Beijing. Surnommé le « MIT chinois », il s'agit de l'une des meilleures universités de recherche technique en Chine et dans le monde. Les capacités cyber offensives de ses étudiants sont particulièrement connues grâce à *Blue-Lotus*, une compétition entre les équipes de recherche de haut niveau sur la cybersécurité. Le rapport révèle aussi que le bureau de la recherche scientifique et du développement de l'Université *Tsinghua* a participé en mai 2018 aux activités préparatoires pour la réunion du parti communiste chinois, au cours desquelles ils ont discuté de la coopération stratégique entre entreprises et instituts de recherche au service du développement du pays.

De façon générale, les universités chinoises ont souvent été associées aux cyber-opérations commanditées par l'État chinois, directement et indirectement. En 2015 par exemple, l'infrastructure APT17 (une cyberarme) a été remontée jusqu'à un professeur de la *Southeast University* de Chine. De même, plusieurs sources rapportent qu'en 2017 l'armée chinoise se serait associée à l'Université *Xi'An Jiaotong* pour créer un programme de cyber milice.

Les données analysées dans le rapport montrent une nette augmentation des activités de reconnaissance réseau (première étape d'une attaque cyber) en provenance de l'université de *Tsinghua* vers les organisations kényanes, avec un pic deux semaines à peine après l'annonce par le Kenya de son intention de ne pas soutenir l'accord de libre-échange Chine-CAE.

La "nouvelle route de la soie" de la Chine et ses investissements à long terme dans les infrastructures africaines la pousse à exercer une influence considérable dans les pays visés par ces politiques. Ainsi, malgré la difficulté d'attribuer la source d'une attaque cyber avec certitude, il est fort probable, comme l'indique la conclusion du rapport sur à son investigation technique, que ces vastes activités de reconnaissance réseau émanant des infrastructures de l'Université *Tsinghua* et visant des intérêts économiques au Kenya (mais aussi Mongolie et Brésil), ont bien été pilotées par l'État Chinois.

Cyberespionnage Chinois vu des USA

La désormais célèbre *affaire Huawei*, symbole contemporain d'affrontements à la fois technologique, économique et informationnel entre la Chine et les Etats-Unis, continue de faire couler beaucoup d'encre et de salive. Même le président Russe *Vladimir Poutine*, reconnu pour sa retenue et ses prises de parole très calculées sur les questions internationales, a pourtant gratifié l'opinion mondiale de cette déclaration sur le sujet : « *L'attaque contre Huawei, d'où vient-elle et quel est son but ? Il n'y a qu'un seul objectif : celui de freiner le développement de*

la Chine qui est devenue le concurrent global d'une autre puissance mondiale, les États-Unis[3] ».

Au-delà de cette affaire, plusieurs services américains ont souvent dans leurs rapports accusés la Chine de cyberespionnage massif contre bon nombre d'entreprises dans le monde pour des raisons économiques (secrets technologiques et industriels). Tant et si bien que le 17 décembre 2018, le département américain de la justice a pointé du doigt deux diplomates chinois vivant aux USA (*Zhang Jianguo* et *Zhu Hua)*, les qualifiant de « cyberespions » appartenant au groupe de hackers chinois APT10. D'après la fiche de recherche du FBI, ils ont été inculpé de « *complot pour intrusion informatique, de complot pour fraude électronique et d'usurpation d'identité aggravée* », pour avoir mené des attaques cybernétiques entre 2006 et 2018 contre la NASA, l'US Navy et bien d'autres grandes entreprises du secteur aéronautique, à la demande du ministère de la sécurité publique chinois.

Selon les experts des services de renseignement américains, leurs homologues chinois auraient mené plus récemment en 2017 une cyber-opération au nom de code "***Cloudhopper***", en violation des accords de 2015 sur le cyberespionnage signe entre *Xi Jinping* et *Barack Obama* afin de calmer les tensions entre les deux sur ce sujet. L'opération *Cloudhopper* avait vraisemblablement pour cibles les réseaux de HP et IBM dans le monde, avec pour finalité d'accéder aux informations des clients de ces deux géants fournisseurs de services d'hébergement sur le Cloud. Bien entendu le gouvernement de Pékin, par le biais de son ministère des Affaires étrangères, accuse de son côté les USA de diriger à grande échelle un réseau de vol de données et surveillance de masse.

Un rapport encore plus récent inquiète les services étatsuniens. Rendu public le 20 Mai 2020 par la fondation américaine *The Heritage Foundation*, il révèle l'espionnage massif de plusieurs bâtiments officiels en Afrique par le gouvernement chinois, menaçant ainsi les intérêts américains sur le continent. *Joshua Meservey*, auteur de ce rapport adressé à l'état fédéral américain, fait remarquer de prime abord que « *Pékin pourrait avoir un meilleur réseau de surveillance en Afrique que partout ailleurs dans le monde* ». Cet analyste rappel qu'au nom des multiples accords de coopération entre les pays africains et la Chine, et au regard de la stratégie de cette dernière sur le continent noir, « *les entreprises chinoises ont construit ou rénové (ou les deux) au moins 186 bâtiments gouvernementaux africains sensibles ; les entreprises chinoises de télécommunications ont construit au moins 14 réseaux de télécommunications intra-gouvernementaux "sécurisés" ; et le gouvernement chinois a fait don d'ordinateurs à au moins 35 gouvernements africains* ».

Aligné sur la position officielle de son pays qui considère la Chine comme le leader mondial des opérations d'espionnage économique et d'influence étrangère, *Joshua* postule que « *Pékin utilise presque certainement ses engagements en Afrique pour surveiller les fonctionnaires et les chefs d'entreprise américains et africains. Le gouvernement chinois pourrait*, selon lui, *utiliser les informations qu'il recueille pour avantager ses entreprises en concurrence avec les*

[3] Déclaration faite le 20 Juin 2019 lors de la séance annuelle des questions réponses aux médias.

entreprises américaines et autres, glaner des informations sur les programmes américains d'aide à la sécurité et de lutte contre le terrorisme, et recruter ou influencer de hauts fonctionnaires africains ».

Offensive des Etats-Unis contre la Chine sur la 5G, une leçon de guerre au 21ème siècle

L'une des initiatives les plus récentes du gouvernement américain pour la protection de son cyberespace et visant principalement à contenir le rival chinois, c'est la création de tout un programme baptisé « réseau propre » (*Clean Network Program*). Le but déclaré de cette démarche est de protéger la vie privée des américains et les informations les plus sensibles de leurs entreprises contre les intrusions agressives d'acteurs malveillants, notamment et particulièrement le Parti Communiste Chinois (PCC) que Washington considère comme ennemi public numéro 1 en matière de cyberespionnage. Pour les stratèges du pentagone et de la NSA, l'atteinte de ce but passe par la construction d'un réseau de communication et d'échange d'information (dans les Etats-Unis ainsi qu'avec leurs alliés) qui échappe complètement à l'utilisation des technologies chinoises, jugées dangereuses pour les intérêts étatsuniens.

Il faut dire que cette réaction correspond aussi aux activités du gouvernement chinois (dont nous avons décrit quelques-unes *supra*) et son ambition telle que perçue par la Maison Blanche. En effet, on assiste à un affrontement entre deux puissances qui ont théorisé leur domination du monde par les technologiques numériques et le cyberespace. Cela s'est manifesté au cours des dernières années par des milliers de cyberagressions de part et d'autre, chacun contre les intérêts de son rival. Cependant, du côté des Etats-Unis, la dénonciation publique des attaques subies fait partie de la stratégie de riposte, ce qui bien entendu n'exclut pas les opérations offensives des américains dans le cyberespace, comme nous l'a rappelé Snowden. Mais cela explique pourquoi la Chine est régulièrement pointée du doigt dans les médias comme champion du cyberespionnage tel que nous l'avons illustré précédemment.

En 2012 par exemple, le gouvernement américain avait confirmé dans une communication officielle que l'un des réseaux les plus critiques pour la sécurité de l'Etat (réseau militaire de la Maison Blanche qui permet entre autre l'accès aux commandes nucléaires) avait fait l'objet d'une cyberattaque menée depuis la Chine[4]. Cette cyberattaque intervenait suite à une manœuvre militaire du pentagone dans les eaux japonaises proches de l'île Senkaku, dans un contexte de tension entre la Chine et le Japon qui se disputent ce territoire. En attaquant ainsi le cœur du pouvoir américain, la Chine ne fait aucun mystère de ses intentions : riposter lorsque ses intérêts sont menacés, et devenir la première puissance mondiale devant les Etats-Unis.

La rivalité entre ces deux géants trouve aujourd'hui son point culminant sur la technologie sans fil de cinquième génération (5G). En effet, au regard des enjeux et des implications escomptées de la 5G considérée par les spécialistes comme une technologie de rupture et du futur (pour ses

[4] Bill Gertz, *White House Hack Attack*, FreeBeacon.com, Septembre 2012

usages industriel et militaire notamment), chaque partie est convaincue que sa maîtrise lui donnera une position dominante dans les prochaines décennies. Mais pour le pays de l'oncle Sam le défis est de taille, étant donné l'avance factuelle et reconnue de la Chine.

Le Dr Maurice SIMO DJOM, chercheur en intelligence économique, l'illustre clairement dans un article[5] récent en ces termes : « *Le décrochage technologique a été mis à jour récemment. On a appris que les équipementiers américains ne sont pas à la pointe de la 5G alors qu'en face, Huawei totalise 80.000 chercheurs, carbure à un budget de 15 milliards de dollars et déclare pas moins de 3325 familles de brevets 5G ! Au même moment, les américains Qualcomm et Intel réunis n'en déclarent que 2264. Soit dit en passant, ZTE, un autre équipementier chinois affiche 2204 brevets déclarés. Ce qui fait des Chinois les premiers dans la course à la 5G devant les Sud-Coréens : Samsung et LG totalisent 5309 familles de brevets. (Données de décembre 2019)* ».

D'où la cristallisation récente des affrontements sur la question, et surtout la forte agressivité étatsunienne qui ne lésine sur aucun moyen : guerre informationnelle, guerre économique et commerciale, rapports de force diplomatique, etc. C'est d'ailleurs pourquoi selon la nouvelle stratégie américaine, la toute première initiative du programme « réseau propre » est la nécessité de contenir la domination chinoise sur la technologie 5G. Annoncé dans un point de presse en avril 2020, le « *5G Clean Path* » représentait donc la première phase de ce vaste programme. Au-delà de l'objectif affiché qui est de sécuriser les données circulant sur les réseaux 5G en provenance ou à destination des USA, il s'agit pour le département d'Etat de construire une coalition d'acteurs (alliés, partenaires gouvernementaux, industriels et opérateurs de télécom du monde entier, etc.) autour du boycott des technologies chinoises, pour des raisons de sécurité nationale !

On peut trouver là des éléments expliquant pourquoi dans une communication officielle[6] datant de Mai 2020, *Huawei* est dépeint comme « un constructeur indigne de confiance et un outil à la solde du Parti Communiste Chinois ». Ce communiqué révèle que le ministère américain de la justice a inculpé *Huawei* pour avoir volé des technologies américaines et aidé l'Iran à se soustraire aux sanctions. Il nous apprend aussi que Washington par la voie de son ministère du commerce a placé ce géant du numérique sur sa liste noire en 2019 (l'empêchant ainsi de faire des affaires avec les entreprises américaines).

Conséquence, plusieurs pays tels que le Royaume-Uni, la République tchèque, la Pologne, la Suède, l'Estonie, la Roumanie, le Danemark, la Lettonie et la Grèce ont ainsi déjà rejoint cette coalition en adoptant d'autres constructeurs (l'européen ERICSSON par exemple) pour développer leur infrastructure 5G. Toutes ces actions visent aussi à casser la dynamique de la

[5] Dr Maurice Simo Djom, *Projections : les 5 figures du monde post-coronial*, Economie du cameroun, 2020

[6] Michael POMPEO, *Les États-Unis protègent la sécurité nationale et l'intégrité des réseaux 5G*, communiqué de presse du Secrétariat d'Etat Américain, Mai 2020.

Chine dans la construction de sa « route de la soie digital », pour laquelle la technologie 5G et l'opérateur Huawei occupe un rôle central.

Conscient cependant du fait que la maîtrise du réseau 5G ne suffirait pas pour contrer la puissance chinoise et garantir les intérêts stratégiques des Etats-Unis et ses alliés, l'administration TRUMP à décider de passer à la vitesse supérieure ! C'est ainsi que dans un autre communiqué de presse[7] datant du 5 Août 2020, le secrétaire d'Etat Américain Michael POMPEO a annoncé l'extension du programme « réseau propre ». Cette annonce portait sur le lancement de cinq nouvelles lignes d'action visant à renforcer le dispositif, notamment par la protection des infrastructures technologiques et de télécommunications essentielles au fonctionnement des États-Unis.

En plus du dossier de la technologie 5G, les cinq nouveaux piliers de ce réseau de confiance relevés dans l'annonce en question portent sur les points suivants :

Clean Carrier (transporteur propre) : Le but est de s'assurer que les communications en provenance et à destinations des Etats-Unis soient traitées par des opérateurs de télécom fiables, c'est-à-dire capables de remplir leur mission sans utilisation des technologies d'acteurs jugés malveillants tels que la Chine.

Clean Cable (câblage propre) : Il est question ici de veiller à ce que les câbles sous-marins reliant les Etats-Unis au reste du monde (l'internet) ne soient pas détournés ou compromis à des fins de collecte de renseignements par les ennemis des intérêts américains.

Clean Cloud (Cloud propre) : L'objectif est d'empêcher que les données personnelles et sensibles des américains, ainsi que la propriété intellectuelle et industriel des entreprises étatsuniennes ne soient stockées et traitées par des prestataires de services Cloud jugés peu fiable. Les entreprises clairement visées ici sont *Alibaba, Baidu* ou *Tencent* qui sont les seuls à pouvoir rivaliser avec les géants américains leaders du marché mondial, mais considérées comme inféodées au gouvernement chinois.

Clean Store (boutique propre) : L'idée est de détecter et supprimer les applications non fiables publiées dans les boutiques d'applications mobiles américaines (notamment Google PlayStore et Apple Store). D'après le gouvernement américain, plusieurs applications mobiles d'origine chinoise menacent la vie privée de ses citoyens sur leurs Smartphones par la prolifération des virus, le vol d'information, la propagation des messages de propagande ou de désinformation, etc.

Clean Apps (applications propres) : Cet axe vise à dissuader les grandes entreprises américaines et étrangères du numérique, de mettre à disposition pour téléchargement ou d'autoriser la pré-installation de leurs applications mobiles sur les Smartphones de fabricants jugés non fiables. Pour le gouvernement américain, ces entreprises devraient retirer leurs applications de la boutique des fabricants tels que Huawei (considéré par Washington comme une branche

[7] Michael POMPEO, *Annonce portant extension du "réseau propre" pour la sauvegarde des actifs américains*, communiqué de presse du Secrétariat d'Etat Américain, Août 2020.

technique du renseignement chinois) afin de s'assurer qu'elles ne sont pas associées à un acteur dangereux.

C'est donc en cela que consiste le programme "*Clean Network*", qui connaît un essor de plus en plus croissant et qui est délibérément agressif vis-à-vis de la Chine ! Ainsi, la puissance américaine a pesé de tout son poids pour que plus d'une trentaine de pays et territoires s'engagent à utiliser exclusivement des « fournisseurs de confiance » pour leurs réseaux de communication, ce qui en fait désormais des « Pays Propres » aux yeux des Etats-Unis. De plus, beaucoup des plus grandes entreprises de télécommunications dans le monde, toujours sous influence étasunienne, ce sont elles aussi désormais rangées dans la catégorie des « Télécom Propres » qui fait partie du même programme.

En générale quand on veut parler de souveraineté numérique, les pays tels que la Russie, l'Iran ou encore la Chine sont les plus régulièrement cités par les spécialistes comme ayant théorisées puis mise en pratique ce concept, en construisant leurs propres modèles et leurs réseaux nationaux pour échapper au modèle et à la domination occidentale dont l'Amérique est le porte étendard. Avec cette initiative « réseau propre » qui prône clairement une forme de protectionnisme technologique, il est désormais évident qu'en dehors de toute propagande, la souveraineté numérique est au cœur de la stratégie américaine dans le cyberespace. Michael POMPEO, Secrétaire d'Etat de Donald Trump, le confirme lors d'un point de presse d'Avril 2020 il a déclaré ceci : « *…tout comme l'administration Trump a pris des mesures sans précédent pour défendre nos frontières physiques, nous défendons également l'Amérique sur les cyber-frontières* ».

Quelles leçons pour l'Afrique ?

Au regard de la guerre économique et informationnelle sans merci que se livrent ainsi les USA et la Chine, le projet de la route de la soie prend une dimension stratégique particulière. En fait, cette brève analyse des rapports de force (notamment avec l'exemple de la 5G) entre la Chine (qui est ralenti dans son élan d'étendre le déploiement de cette technologie sur l'étendue de la route de la soie numérique) et les Etats-Unis (qui use de son influence sur ses alliés européens afin de bloquer l'initiative chinoise) nous laisse entrevoir que le prochain théâtre d'affrontement de ces puissances pourrait bien être le continent africain.

Les faits récents ne semblent pas démentir cette tendance, notamment avec l'empire du milieu qui ne lésine sur aucuns moyens pour étendre et consolider son positionnement sur le continent, y compris donc ses moyens numériques connus pour être très avancés. Car vous l'avez compris, il s'agit bien de la bataille pour devenir première puissance mondiale ! A la suite des révélations de 2018 sur le cyberespionnage au siège de l'Union Africaine, le cas du Kenya évoqué ici est une piqûre de rappel et n'est qu'une illustration de ce que subissent certainement la plupart des pays Africains où la Chine est présente, comme en témoigne d'ailleurs le rapport de la fondation *The Heritage Foundation* que nous venons d'évoquer.

Pourtant, malgré tous ces évènements, les pays et organisations africaines continuent d'accentuer la coopération avec la Chine et ses géants technologiques. En effet, en Mai 2019,

l'Union Africaine a signé un nouveau protocole d'accord avec le mastodonte chinois Huawei, en vue de renforcer le partenariat technique des deux parties et ce sur cinq domaines bien précis : l'intelligence artificielle (AI), l'internet des objets (IoT), la technologie 5G, les infrastructures de haut débit et le Cloud Computing (via la construction des centres de données). Ce nouvel accord, qui permet à la Chine de négocier de façon bilatérale avec chaque pays africain (profitant ainsi de leur fragilité pour imposer ses normes technologiques), vient consolider sa position dans les secteurs stratégiques sur le continent. Ce qui bien entendu nourrit les inquiétudes des autres puissances présentes sur le terrain, comme en témoignent les différents rapports américains.

Depuis quelques années déjà, la présence de Huawei se faisait ressentir dans plusieurs pays à travers divers projets d'infrastructure haut débit, de ville intelligente (Smartcities), de construction de centres d'hébergement de données (datacenter), etc. (exemple du cœur des réseaux de télécommunications Camerounais et Egyptien, système de vidéosurveillance avec analyse des données dans les pays comme la Tanzanie, le Kenya ou la Zambie, installation des centres de données au Ghana, en Afrique du Sud, à Djibouti, etc.). A l'analyse, cette démarche de mise sous tutelle technologique progressive et de maîtrise des données au prétexte d'une nouvelle forme de partenariat sud-sud, dépasse largement le cadre économique pour s'inscrire dans une logique d'encerclement inhérente au projet de la route de la soie numérique, et propre à la pensée stratégique chinoise (jeu de go). ***Cf. image 2 et 3 ci-dessous***.

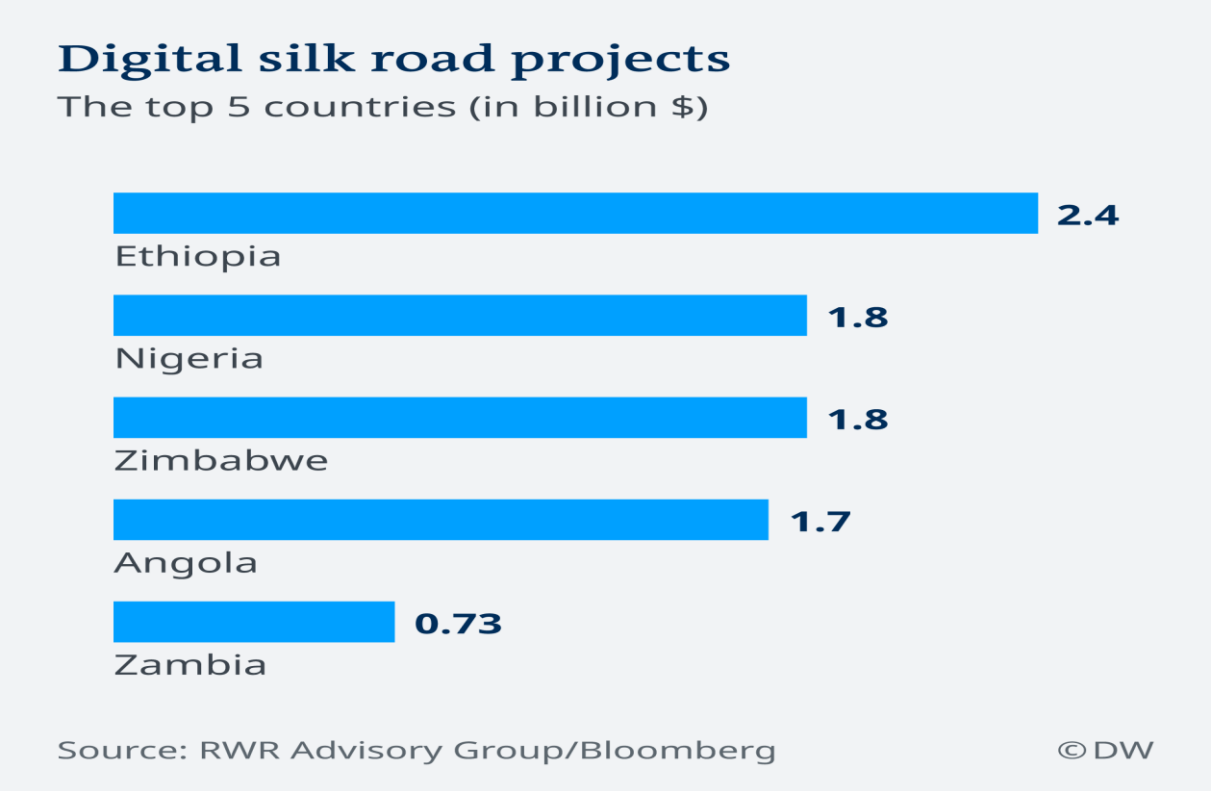

Image 2 : Pays africains premiers bénéficiaires des projets de la route de la soie numérique

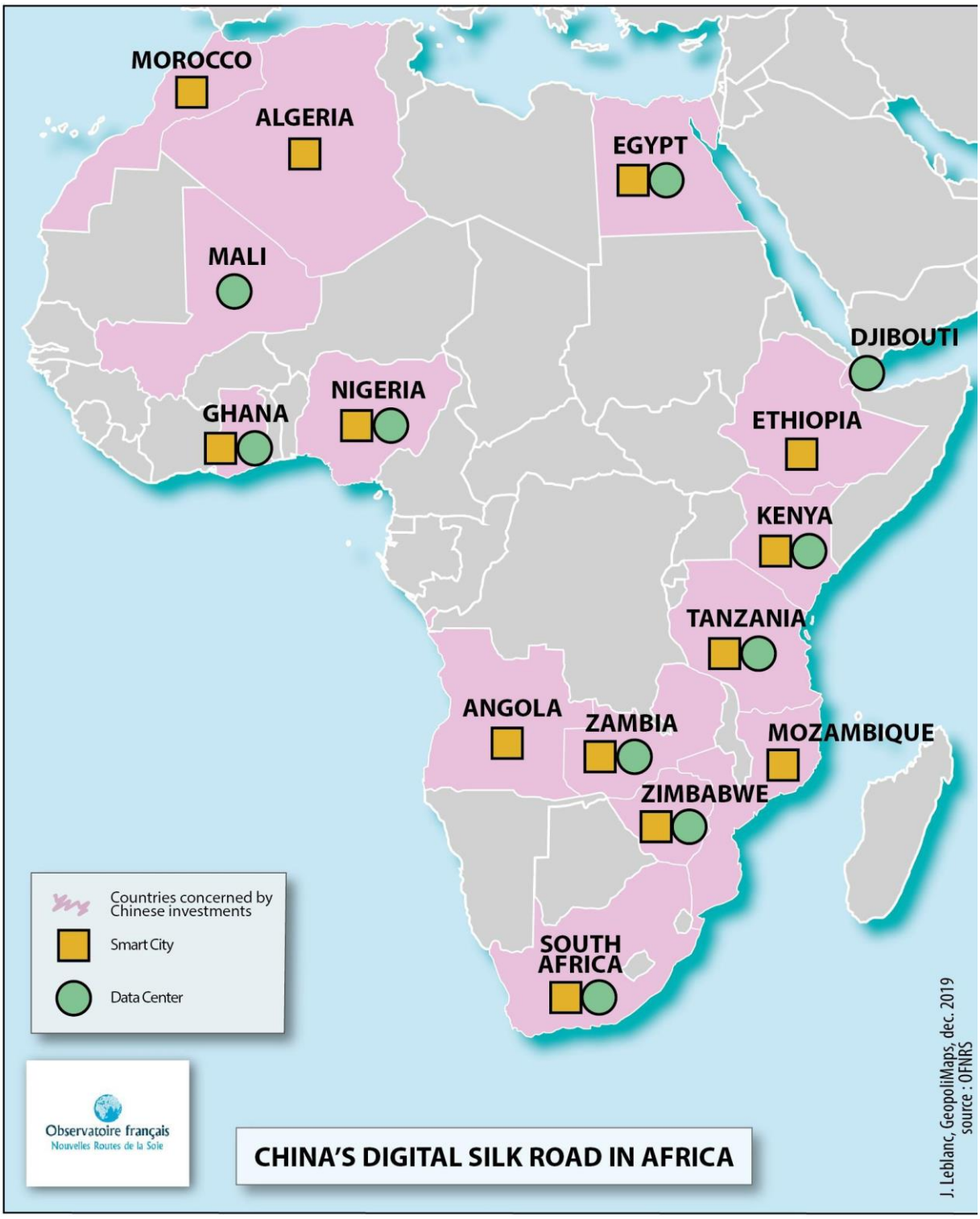

Image 3 : Route de la soie numérique en Afrique

Au-delà du parti pris évident pour les intérêts américains, les deux rapports (*Recorded Future* et *The Heritage foundation*) que nous avons exploré devraient tout de même attirer l'attention des africains sur la nécessité de changer de paradigme dans l'accès aux technologies et la protection de leurs infrastructures numériques. Au regard de la complexité et l'intensité des nouvelles cybermenaces, ainsi que des affrontements entre puissances sur leur territoire, il revient aux pays africains d'élaborer une stratégie endogène et de développer leurs propres capacités de cyberdéfense pouvant y faire face, afin de maintenir une coopération sereine, équilibrée mais surtout souveraine avec la Chine ou toutes les autres puissances.

Ce n'est qu'en adoptant une telle démarche qu'il apparaîtra évident à nos états de toujours inspecter les dispositifs de communication installés dans les bâtiments reçus en cadeau, de ne jamais installer des solutions technologiques étrangères (matériel et logiciel) dans des infrastructures sensibles sans une homologation préalable par nos propres experts, de promouvoir l'émergence d'une industrie africaine de cybersécurité et de cyberdéfense, etc.

C'est exactement cette thèse que je développe en détail dans mon ouvrage intitulé *« Souveraineté numérique et cyberdéfense : un enjeu de taille pour l'Afrique »*, dans lequel je suggère quelques pistes de réflexions et de solutions pouvant influencer les choix stratégiques et inciter au développement des mécanismes plus efficaces afin de protéger l'espace cybernétique Africain.

A propos de l'Auteur :

DJIMGOU NAGMENI est Entrepreneur, Conférencier, Consultant international en cybersécurité / cyberdéfense, Enseignant à l'École Politique Africaine de Paris, Spécialiste de cyberstratégie et Fondateur du LARC.

A 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, « Route de la soie numérique et affrontements Chine-USA : les enjeux pour l'Afrique », Note n°05 - LARC, Avril 2021.