Laboratoire Africain de
Recherches en Cyberstratégie

Comprendre le Cyberespace : un impératif pour l'Afrique!

Par DJIMGOU NGAMENI

Mars 2021

Résumé :

Au regard de sa centralité dans le fonctionnement des sociétés modernes, le cyberespace en tant que concept fait l'objet d'une étude approfondie par la plupart des pays dans le monde, à l'exception des Etats africains. En effet, rare sont les documents officiels, les études universitaires, les livres ou autres publications des africains à propos des TIC et du numérique qui commencent par définir rigoureusement ce concept. Tant qu'une réflexion sérieuse sur ces aspects n'est pas engagée sur le continent, il sera très difficile pour nos dirigeants de comprendre la cyberguerre (et les moyens qui l'accompagnent) telle qu'elle se déroule aujourd'hui, aussi bien dans nos pays que dans le reste du monde.

Introduction

Le cyberespace en tant que concept est devenu un objet d'étude scientifique. Tout le monde l'a compris, sauf l'Afrique ! En effet, rares sont les documents officiels, les études universitaires, les livres ou autres publications des africains à propos des TIC et du numérique qui commencent par définir rigoureusement ce concept. Alors qu'ailleurs des centres de recherche pluridisciplinaires se sont penchés sur la question depuis la fin des années 1990, l'Afrique se complait dans une approche superficielle et par conséquent, incomplète.

Cet impensé est très probablement l'un des principaux facteurs expliquant la limite de nos stratégies de transformation numérique sur le continent, qui malgré elles entretiennent notre dépendance technologique vis-à-vis des grandes puissances. Ne pas comprendre le cyberespace dans toute sa complexité, ne pas l'interroger à partir de nos propres grilles d'analyse, nous condamne à ne pas tenir compte de toutes les implications (stratégique, politique, économique, etc.) qui en découlent. C'est habité par cet impératif que je propose, sur la base des études existantes, une première lecture approfondie du cyberespace, sans laquelle il n'est pas possible de penser une cyberstratégie africaine cohérente et opérante.

La genèse du cyberespace : chronologie historique

Comme il est désormais coutume de le rappeler, le mot « *cyberespace* » a été utilisé pour la première fois dans un ouvrage intitulé *Neuromancer*, œuvre littéraire de science-fiction publié en 1984 par *William Gibson.* Pour choisir cette appellation, *Gibson* s'est inspiré du concept de « *cybernétique* » qui serait initialement inventé par le mathématicien Français *André-Marie Ampère* [1834], mais mieux connu plus tard dans les travaux du mathématicien Américain *Norbert Wiener*, suite à la publication en 1948 de son livre du même titre[1]. Cependant, dans un article dédié à cet effet[2], nous avons clairement montré que le terme « *cybernétique* », quel que soit la signification qu'on donne au mot grec [*kubernêsis, Kubernêtikê*] dont il découle, puise son origine étymologique dans la civilisation égypto-nubienne. Oui, le concept de *cybernétique* a une étymologie africaine !

Dans son ouvrage devenu culte, *William Gibson* (par ailleurs fondateur du mouvement cyberpunk[3]) définit le cyberespace comme étant *« une hallucination consensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts des mathématiques… ».* Si cette description du cyberespace semble plus relever d'une expérience de pensée qu'autre chose, *Gibson* dans ce même livre en propose une autre qu'on pourrait dire plus « prémonitoire ». Il évoque *un espace tridimensionnel d'une « infinie complexité », généré électroniquement, dans lequel ses personnages entrent en se connectant par ordinateur.*

---

[1] Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, 1948

[2] François-Xavier DJIMGOU, *Des origines africaines du « cyber », 2020*

[3] Issu de la confluence entre les mots *cybernétique* et *punk* (ou hacker et rocker), le cyberpunk est un genre particulier de science-fiction qui met souvent en scène un futur proche empreint de violence et de pessimisme, avec une société technologiquement avancée.

Il s'agit là d'une représentation mentale des données et de l'information stockées au cœur des systèmes informatiques de toute l'humanité, qui va alimenter des mouvements tels que le cyberpunk, et dont vont s'approprier des générations d'internautes. Mais surtout, cela va servir de base aux pionniers du réseau internet qui vont s'en inspirer pour le concevoir et le développer à l'origine comme un espace de liberté et d'ouverture, décentralisé, autogéré, etc. C'est ce qui transparait par exemple dans la « *déclaration d'indépendance du cyberespace* », texte publié en 1996 par un membre de la *Electronic Frontier Foundation (EFF)*[4].

De la fiction à la réalité…

Mais rappelons qu'à ce stade le cyberespace relève de la science-fiction, écrit par un romancier ! Au cours des années 90, la plupart des pays ont procédé à l'installation massive des infrastructures de communications afin de suivre l'initiative américaine, qui domine la construction des réseaux depuis le projet *Arpanet* en 1969 jusqu'aux débuts d'Internet à partir des années 1990. Cela a abouti à l'expansion de la connectivité à travers le monde, avec l'impact exponentiel qu'on a connu sur toutes nos activités quotidiennes.

Mais en dehors des petits cercles de spécialistes de science-fiction ou des membres de l'*EFF*, le terme *cyberespace* était ainsi provisoirement tombé aux oubliettes pour le reste du monde. On parlait alors de nouvelles technologies de l'information et de la communication (NTIC), pour désigner ce réseau d'infrastructures technologiques qui a permis l'échange des volumes de plus en plus important de données, créant progressivement la société de l'information.

Cette expansion du réseau a généré progressivement de nouveaux risques et de nouveaux comportements (cybercriminalité) avec un pic à la fin des années 1990. C'est précisément à cette période-là que le terme *cyberespace* revient dans le débat public ! En effet, suite à l'attentat commis par *Timothy McVeigh* dans l'*Oklahoma* aux États-Unis en 1995[5], le président américain de l'époque *Bill Clinton* a créé un groupe de travail connu sous le nom de CIWG (*Critical Infrastructure Working Group*). C'est dans ce cadre que les membres dudit groupe vont intégrer la sécurité des systèmes informatiques dans le périmètre des infrastructures critiques de leur pays. Parmi eux, le juriste *Michael Vatis* travaillant pour le DoJ (Département américain de la Justice) et qui venait de lire le roman de *Gibson*, a proposé l'usage du terme « *cyberespace* » pour désigner l'ensemble de tous les systèmes informatiques interconnectés des États-Unis. Ce qui fait de lui le premier à l'employer dans un contexte « officiel ».

A sa suite, le terme sera repris partout dans le monde et va rester dans le langage commun. On le retrouve notamment dans le discours des Etats qui face aux nouvelles menaces engendrées par les réseaux, le désigne pour la première fois comme un *territoire* au sens géopolitique : c'est-à-dire un espace à conquérir, à délimiter, à surveiller et surtout à contrôler. De nos jours, on retrouve ce terme partout : l'influence du cyberespace ayant continué à grandir dans tous les domaines de la vie d'une nation (y compris le domaine militaire...).

Tout ceci a conduit les Etats-Unis, par la voix de son secrétaire d'état à la défense de l'époque William J. Lynn III, à reconnaître publiquement le cyberespace dès Septembre 2010 comme " *"le cinquième domaine de la guerre"*" au même titre que la mer, l'espace, la terre et l'air.

[4] L'*Electronic Frontier Foundation* est une ONG de protection des libertés sur Internet créée aux USA en 1990. *John Perry Barlow*, un de ses membres, y a publié la « Déclaration de l'indépendance du cyberespace ».

[5] L'attentat d'Oklahoma City est un acte terroriste perpétré le 19 avril 1995 par *Timothy McVeigh* avec un véhicule piégé à l'explosif, visant le bâtiment fédéral *Alfred P. Murrah* et causant la mort de 168 personnes et plus de 680 blessés. (Source Wikipédia).

Pionniers de cette démarche, l'État américain a très vite revu sa stratégie de contrôle et d'influence dans ce nouvel espace, et a développé de nouvelles cyber-capacités (offensives et défensives) pour la mettre en œuvre. La Chine et la Russie n'ont pas tardé à faire de même, ainsi que la France qui dans son *Livre blanc sur la défense* en 2013, marque un tournant décisif en indiquant explicitement que "*le cyberespace est une priorité stratégique et les armes cybernétiques font désormais partie de l'arsenal*". En Juillet 2016, ce sont les membres de l'OTAN qui dans une déclaration officielle reconnaissent le cyberespace comme « théâtre d'opérations dans lequel ils doivent également se défendre. Ce qui, bien entendu, appelle à un développement de capacité cyber (offensive et défensive) pour y parvenir efficacement. Ainsi, loin du « village global » dont les plus naïfs rêvaient (les africains notamment), le cyberespace est bel et bien un champ de conflits et un espace d'affrontement.

A quoi renvoi le Cyberespace de nos jours ?

Rendu 30 ans plus tard, l'usage du terme *cyberespace* renvoie bien souvent à des réalités différentes. Pour les profanes il fait essentiellement référence à internet, ce grand réseau public qui permet la circulation de l'information. Certains experts le définissent comme étant un *espace "virtuel" constitué par l'ensemble des réseaux (réseau public internet et réseau privé intranet) interconnectés*. Pour l'ANSSI en France (Agence Nationale de la Sécurité des Systèmes d'Information) par exemple, c'est « *l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées* ». C'est cette définition de l'ANSSI qui est très paresseusement reprise et utilisée par certains pays d'Afrique francophone dans leurs textes officiels.

Hors à l'analyse, même si ces définitions (très orientées technique et technologique) reflètent une part de réalité, le cyberespace est un concept dont les contours restent assez flous au regard de l'usage qui en est fait par le grand public. Plusieurs chercheurs, experts, universitaires et même États major militaires dans le monde étudient d'ailleurs très rigoureusement la question en adoptant des approches parfois inattendues. Le politologue Canadien *Hugo Loiseau* par exemple, l'aborde du point de vue sociologique. Selon lui, « *le cyberespace c'est la mise en réseau d'une représentation modifiée des activités humaines sous forme numérique et virtuelle* ». Nombres d'études tendent aussi à explorer voir démontrer une analogie (au moins conceptuelle) entre le cyberespace et l'espace maritime afin de mieux le comprendre, de pouvoir ainsi l'expliquer et surtout le réglementer[6]. Il convient donc de constater que c'est une notion difficile à appréhender.

En l'état actuel des travaux disponibles, plusieurs remarques s'imposent : On note premièrement qu'il n'existe pas à ce jour une définition universelle et consensuelle du cyberespace. Aussi bien aux USA qu'en France, en Russie, en Chine, en Israël, etc., à défaut d'une définition, il existe différentes *représentations* du cyberespace, chacun le concevant comme une projection de ses propres valeurs civilisationnelles et en fonction de ses intérêts stratégiques. Chaque acteur du cyberespace (Etats, individu, groupes organisés, etc.) en a ainsi sa propre "représentation" au sens du géographe Français *Yves Lacoste*, entendu comme « *ensemble d'idées plus ou moins logiques et cohérentes associé, et qui décrit, exprime une partie de la réalité, de façon floue ou précise, déformée ou exacte* ».

[6] Cf. l'étude confiée en 2013 par la DAS (Délégation aux Affaires Stratégiques) à la Compagnie Européenne d'Intelligence Stratégique (CEIS) sur le thème : « *Les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ?* ».

Au final on a un système complexe de représentations parfois contradictoires qui s'enchevêtrent, s'agrègent et s'opposent, ce qui est probablement l'une des raisons pour lesquelles il est difficile de dégager une définition consensuelle. On a par exemple la représentation européo-centrée qui renvoie à un espace d'expression des libertés, de démocratie, etc., tandis que celle de la Chine et de la Russie se caractérise par un *espace informationnel* contrôlé et maîtrisé. Pour la plupart des pays africains (qui ont tous un déficit de réflexion théorique sur la question), le cyberespace continue à être perçu comme ce vecteur de développement économique et social, qui nous propulse dans la mondialisation en nous donnant accès à un illusoire beau village global et planétaire…

Dans le cas des Etats-Unis, il est bon de rappeler que le spécialiste américain de géostratégie *Zbigniew Brezinski* avait théorisé la représentation idéologique que les américains se font du cyberespace aujourd'hui. En effet, dans son livre *Révolution technétronique (Calmann-Lévy 1971), Brezinski* considère dès 1970 que la puissance informatique des États-Unis sera le moyen de la victoire sur la puissance soviétique. Cela fait ainsi écho à la course des années 50 - 60 pour le premier homme dans l'espace et sur la lune, dominée technologiquement par l'union soviétique, et catalysée par la guerre idéologique entre capitalisme et communisme.

Au-delà des mouvements étatsuniens qui défendent une certaine idée libertaire qui serait à l'origine de réseau internet, et du discours d'ouverture et de neutralité officiellement porté par les ONG occidentales dans le reste du monde, l'approche idéologique américaine est largement confirmée par plusieurs penseurs. Convaincu de cet état de fait, l'écrivain anglo-pakistanais *Ziauddin Sardar* l'exprime clairement dans ses écrits en ces termes :

« *Le cyberespace n'est pas apparu ... de nulle part... Il est le reflet conscient du désir, des aspirations, de l'aspiration expérientielle et de l'angoisse spirituelle de l'homme occidental ; il est résolument conçu comme un nouveau marché, et est un produit emphatique de la culture, de la vision du monde et de la technologie des civilisations occidentales... le cyberespace, donc, est le rêve américain au sens large ; il marque l'aube d'une nouvelle civilisation américaine... le cyberespace est particulièrement orienté vers l'effacement de toutes les histoires non occidentales.*[7] ».

Martin Dodge, autre chercheur précurseur de la cybergéographie et s'intéressant particulièrement au lien entre les flux de capitaux et les flux de données, est exactement sur la même longueur d'onde que *Sardar*. Pour lui, « *Il est reconnu que le développement et la promotion des TIC et du cyberespace sont liés aux modes de production capitalistes - le cyberespace est un produit commercial à exploiter économiquement, utilisé pour ouvrir un nouveau marché d'opportunité.* ». C'est pourquoi les pays tels que la Russie et la Chine, résistants historiques à la domination de l'idéologie américaine, ont bien intégré cette dimension dans leur propre conception de l'espace numérique.

La seconde remarque qu'on peut noter concerne l'émergence et l'usage massif des préfixes "Cyber" et "e-" (pour électronique), pour tout ce qui renvoie à une action ou une activité dans le cyberespace par le biais d'un appareil électro-numérique. On parle ainsi de cybercafé, cyberattaque, cyberagression, cybercriminalité, cybergéographie, puis de e-commerce, e-gouvernement, e-mail, etc. Chacune de ces notions ont des répercussions plus ou moins importantes en fonction de la compréhension qu'on en a (cas de cyberagression par exemple,

[7] Ziauddin Sardar, « *cyberspace as the darker side of the West* », Future, 1995: pp. 779-81

qui dans les doctrines occidentales peuvent désormais faire référence à un acte de guerre au sens du droit international). Si on peut comprendre et même admettre la nécessité de contextualisation qui motive cette prolifération lexicale, force est de constater qu'on le fait parfois de façon abusive et injustifiée, ce qui participe à brouiller la compréhension.

Caractéristiques du cyberespace

Le cyberespace dispose de certaines caractéristiques sur lesquelles les chercheurs ont un regard plutôt convergent. C'est un milieu hybride par nature. Décidément artificiel et anthropogène (créée par l'homme), il est à priori intangible pour le profane, transverse (qui pénètre tous les autres milieux et tout en interagissant avec eux), universel et extraterritorial, à la fois concret / réel (câbles, ordinateurs, data centres, satellites, etc.) et virtuel / dématérialisé (données, plateformes, code, etc.), dynamique et autonome (car en constante évolution), etc. Les qualificatifs utilisés qui sont parfois contradictoires montrent bien sa complexité conceptuelle, qui dépasse le simple cadre de l'informatique ou de l'Internet.

Parmi ces caractéristiques, trois principales sont souvent retenues par certains spécialistes à la fois pour leur capacité à intégrer les autres, mais surtout pour leurs importantes conséquences stratégiques. Il s'agit de l'universalité, de la dualité et de l'ubiquité du cyberespace.

L'étendu du réseau [Internet] sur l'ensemble du globe (y compris dans l'espace extra-atmosphérique), l'idée qu'il soit ouvert et accessible partout et par tous, le fait que l'accès à Internet et aux technologies numériques soit érigé en droit par les nations unis, confère au cyberespace son caractère *universel* ! Cette cyber-universalité, qui a fortement contribué à l'essor de la mondialisation, peut s'avérer trompeuse d'un point de vue cyberstratégique. Notamment parce que, comme on le verra, les notions de frontières et de limites ont aussi un sens non négligeable dans le cyberespace.

La *dualité* du cyberespace s'observe de plusieurs manières : il est à la fois public et privé, virtuel et réel, tangible et intangible, transparent et opaque, civil et militaire, fixe et mobile, individuel et collectif, etc. Mais surtout, c'est à la fois un espace d'opportunités et d'affrontements de toutes sortes (politique, économique, stratégique, etc.). C'est particulièrement cette dimension, qui a pourtant d'énormes répercussions stratégiques, que les acteurs africains du cyberespace ne perçoivent pas encore dans leurs grilles de lecture, loupant ainsi toute la complexité du sujet. Ce qui conduit nécessairement à des politiques publiques très en dessous des enjeux comme on peut le constater aujourd'hui.

Quant à l'*ubiquité*, cette caractéristique met en évidence la difficulté de localiser avec certitude les acteurs agissant dans le cyberespace, ou plutôt la capacité pour ces derniers à être à plusieurs endroits au même moment. C'est cette propriété qui explique toute la complexité stratégique que revêt la notion d'attribution dans le cyberespace. En effet, en cas de cyber agression sérieuse, il est aujourd'hui très difficile voire impossible de l'attribuer avec certitude (sur la base des preuves techniques) à un acteur, dans une « fenêtre stratégique [8]» pouvant justifier une riposte légitime. C'est l'une des raisons pour lesquelles la plupart des cyberattaques restent très souvent impunies. L'attribution est un sujet majeur sur lequel les cyber- stratégistes se creusent encore les méninges.

[8] Laps de temps suivant une cyber-agression, et au cours duquel l'Etat attaqué peut apporter une riposte légitime, acceptée aussi bien par son opinion publique que par la communauté internationale.

Structure en couche du cyberespace

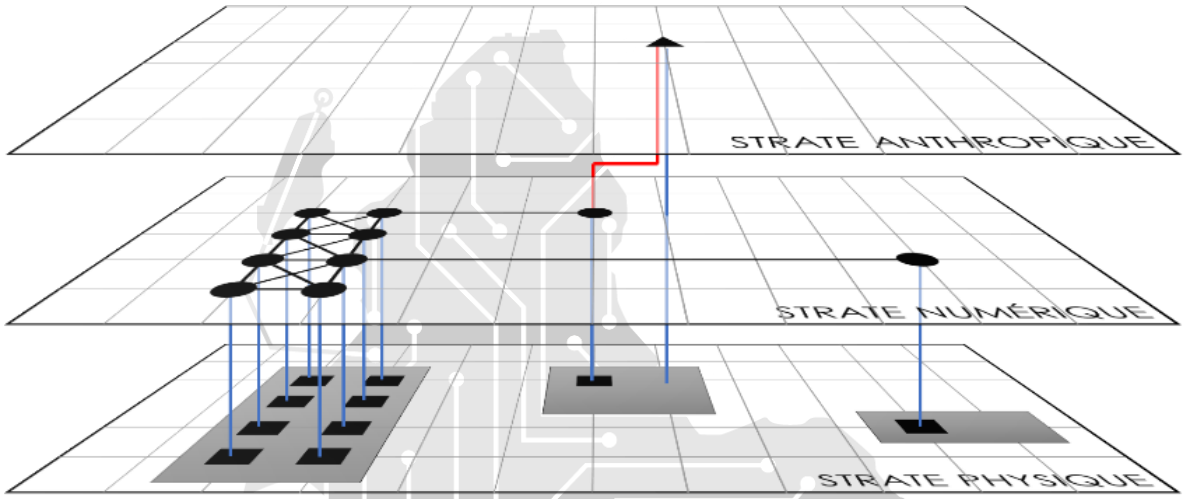
Toujours dans ce souci de description exhaustive et de clarification, de plus en plus de chercheurs abordent la question de « représentation théorique » du cyberespace par une structure en couches, afin de mieux appréhender ses multiples dimensions. On distingue ainsi des modèles à trois, à quatre, voire à cinq couches. Le plus connu et le plus répandu chez les experts est celui à trois couches, initialement proposé vers 2010 par les ingénieurs du département américain de la défense. Il est constitué de :

- *Une couche dite physique ou matériel*, dont les éléments constitutifs sont installés et localisables dans un territoire donné, donc soumis aux contraintes de la géographie physique et politique, sous le contrôle d'un État. La couche physique peut elle-même être divisée en deux grands groupes :
    - les infrastructures d'interconnexion : il s'agit de tout matériel qui permet la connexion au réseau ou l'interconnexion des réseaux entre eux. Notamment les satellites de communication, les câbles sous-marins ou terrestres (fibre optique, cuivre, etc.), les équipements de réseau (routeurs, commutateurs, bornes wifi, etc.), les centres de données, etc.
    - les terminaux : ce sont les appareils d'extrémité tels que les ordinateurs, les Smartphones, les imprimantes, les tablettes, les clés USB, les cartes de crédits, et tout autre élément par lequel un utilisateur final accède ou se sert du cyberespace.

- *Une couche dite logique ou logiciel*, qui est en réalité la couche informatique proprement dite, régie par des programmes sous forme de code et langage compréhensible et utilisable par les machines. Cette couche aussi peut se diviser en deux grands groupes :
    - Le code homme / machine : cela renvoi ici au système d'exploitation des ordinateurs et autres équipements, aux applications / logiciels installés, aux algorithmes de traitement d'information, etc. C'est l'interface qui permet à l'homme d'interagir avec la machine.
    - Les protocoles de communication : cela renvoi à l'ensemble des règles et processus permettant aux différents équipements d'un réseau de communiquer entre eux, d'échanger les informations. Il s'agit notamment du protocole TCP/IP (*Transmission Control Protocol / Internet Protocol*) qui est le plus connu et le plus structurant, le modèle OSI, le protocole DNS, l'adressage et routage IP, etc.

- *Une couche dite Informationnel, sémantique ou psycho-cognitive*. C'est à cette couche qu'est effectuée la création de sens à partir des données transportées sur le réseau, pour en faire une information ou un renseignement. Nous pouvons l'apparenter aux perceptions de la réalité, ainsi qu'au lieu par excellence de gestion des connaissances. On entend ici par « *donnée* » une description élémentaire et codée d'une réalité. Les données additionnées produisent de l'information. Accumulées, on parle de données de masse dit *Big Data*. Si dans une communication le message principal qu'on souhaite transmettre est considéré comme l'information, les données à propos de ce message sont appelées « *métadonnées* » (On les définit aussi comme étant *tout sauf le contenu de vos communications*. Il s'agit par exemple de l'heure, le lieu, la date, la durée de la communication, de l'objet de votre email, etc.) [O. Kempf, 2013].

Dans cette structuration en trois couches, c'est donc cette couche psycho-cognitive qui confère son caractère social au cyberespace. Dans son approche plutôt sociologique du cyberespace telle que nous l'avons évoquée *supra*, l'universitaire canadien *Hugo Loiseau* suggère d'ajouter une quatrième couche dite sociale ou humaine. Au regard des évolutions sociétales profondes observées, c'est une structuration qui va probablement trouver de plus en plus écho chez les spécialistes. Toutes les attaques de type « subversion » (guerre de l'information, manipulation, propagande, encerclement cognitif, etc.), devenues si récurrentes ces dernières années au point de se banaliser, s'opèrent à cette couche.



Structure du cyberespace en 3 couches (source : Conix)

Mais que nous dit cette structuration en couches à propos des limites et des frontières dans le cyberespace ? Peut-on géographiquement situer chaque couche ? Il y a-t-il un rapport entre cette structuration et les attributs géographiques généralement associés au cyberespace ?

Représentations « géographique » du Cyberespace

En plus de la difficulté constatée pour définir le cyberespace et de l'utilisation abusive des préfixes "Cyber" et "e-" pour désigner les actions et activités qui s'y déroulent, il transparaît des travaux les plus avancés sur le sujet que le cyberespace est très souvent décrit en utilisant des attributs spatiaux et géographiques tels que "milieu", "environnement", "domaine", "espace", "monde". D'aucuns parlent même de "territoire", de "cartographie", de "limite", etc. Est-ce à dire que le cyberespace peut effectivement être géographiquement matérialisé ? La question reste entièrement posée… notamment parce qu'au-delà de cette référence commune à la géographie physique, il existe d'autres perceptions géographiques du cyberespace.

Selon *Bertrand BOYER*[9] par exemple, on peut distinguer aux moins deux conceptions de la notion de territoire pour le cyberespace :

La première ***conception dite « classique »*** en référence aux travaux d'*Yves Lacoste*. Pour ce dernier, le territoire a d'abord désigné au Moyen Age un certain nombre de fiefs et de localités sur lesquelles s'étend l'autorité d'un pouvoir ecclésiastique, puis les terres sur lesquelles s'exercent les lois et les pouvoirs d'un Etat. Dès lors, l'Etat fixe, délimite, organise un espace qui par cette intervention se trouve propulsé au rang de territoire. Le problème dans cette

[9] Cf. BOYER B., *Cyberstratégie L'art de la guerre numérique*, Nuvis, 2012.

conception du territoire au sens de la géographie politique est que l'Etat reste au cœur des interactions comme acteur principal, ce qui n'est pas toujours vrai dans le cyberespace où plusieurs autres types d'acteurs entrent en jeu.

La seconde ***conception est dite « éthologique »***, en référence au fonctionnement du règne animal. Celui-ci offre une autre approche de la notion de territoire non plus liée à l'organisation politique, mais plutôt à la hiérarchie sociale. Selon cette approche, le territoire est entendu comme *une zone qu'un animal se réserve, dont il fixe les limites, interdit l'accès à ses congénères et au sein de laquelle il a la plus haute place dans la hiérarchie*. *BOYER* estime que la similitude est plus facile à dégager avec le cyberespace dans ce contexte, étant donné qu'aucun acteur en particulier n'occupe à priori le rôle central. Chaque acteur (individu, états, groupes organisés) a ainsi la possibilité de créer ses propres normes dans cet espace et de l'imposer aux autres, ce qui est d'ailleurs source de tension, de compétition, voire de conflit. C'est une vision qui semble correspondre à un certain fonctionnement du cyberespace, notamment du point de vue des acteurs les plus puissants qui ont une certaine suprématie technologique et normative !

A la suite de *BOYER* nous pouvons évoquer une troisième ***conception dite « multi-spatiale »***, en référence à une tentative d'analogie réalisée entre la mer, l'espace extra-atmosphérique et le cyberespace. En effet la Compagnie Européenne d'Intelligence Stratégique dans une étude (déjà indiquée *supra*[10]) nous propose une approche par le droit, qui permet d'avoir une nouvelle grille de lecture territoriale du cyberespace. Dans cette étude, les chercheurs évoquent un concept « d'entrelacement des espaces » qu'il me semble pertinent d'explorer.

De prime abord, ils remarquent comme *Kavé Salamatian* et *Jérémy Robine*[11] que « *l'espace est une réalité tangible, malgré les moyens les plus modernes de mobilité, tandis que le cyberespace reste intangible pour la plupart de ses utilisateurs* ». Mais par la suite, ils précisent rapidement que cette intangibilité n'est qu'une perception du point de vue de l'utilisateur profane, car l'observation stricte montre que la couche physique[12] du cyberespace est bien ancrée dans les espaces naturels (par exemple, les équipements et centres de données sont dans l'espace terrestre, les câbles sous-marins traversent des espaces maritimes, et les satellites sont au sein de l'espace extra-atmosphérique).

Ce qui traduit bien cet entrelacement du cyberespace et des espaces préexistants, validant ainsi son caractère « transverse ». A l'analyse, il en découle qu'à défaut d'être comparable par leur essence (le cyberespace est un milieu anthropogène quand les autres sont naturels), l'analogie permet tout de même de dégager des similitudes fonctionnelles et stratégiques, et ainsi de transposer certains mécanismes juridiques (responsabilité, libre accès, etc.). L'étude va même jusqu'à évoquer la logique d'aménagement de la souveraineté étatique proposée par le droit de la mer[13], comme hypothèse préférentielle applicable au cyberespace (notamment pour traiter la question de ses frontières).

---

[10] Cf. Note de page No 13.

[11] Kavé Salamatian et Jérémy Robine, « *Peut-on penser une cybergéographie ?* », in « *Cyberespace : enjeux géopolitiques* », Herodote, n°152-153, 2014.

[12] Nous verrons la structuration en couches du cyberespace dans la section suivante.

[13] Extrait du rapport de l'étude : « *Ce droit choisit de morceler la problématique en graduant la portée et l'effectivité de la souveraineté des Etats. Transposé au cyberespace, domaine artificiel, cela équivaut à graduer et donc limiter la portée de la propriété privée en sanctuarisant certaines infrastructures* ».

Même si la *conception classique* du cyberespace comme territoire demeure celle communément admise, ces différentes approches permettront progressivement aux théoriciens de la littérature stratégique africaine de mieux le cerner comme espace d'expression des conflits, ainsi que les nouveaux acteurs et autres rapports de force qui y sont liés. Dans une étude[14] menée en 2015, le professeur *Sébastien-Yves Laurent*, souhaitant se démarquer de la confusion qui peut régner autour des multiples concepts mobilisés (dimension, milieu, espace, etc.) pour rendre compte du cyberespace, a développé la notion *d'environnement cyber* qui semble tout aussi digne d'intérêt. Pour lui, cette expression décrit « *à la fois une réalité spatio-géographique, électro-magnétique, informationnelle et socio-politique* ». Parler d'environnement cyber revient donc à parler de toutes ces réalités en même temps, ce qui me paraît tout à fait enrichissant pour ce travail de clarification. Mais est-ce suffisant pour rendre la notion de cyber plus accessible ?

A la lumière de tout ce qui précède, force est de constater que le cyberespace est un objet d'étude complexe, difficile à cerner. Toutefois, ma conviction est que la meilleure façon de le comprendre et de l'appréhender réside dans une combinaison équilibrée entre ses différentes conceptions comme territoire et sa structuration en couches que nous venons d'explorer, qui tienne en même temps compte de ses caractéristiques spécifiques. Par exemple, si je trouve l'approche par comparaison au « domaine maritime » tout à fait adaptée pour une analogie avec la couche physique du cyberespace, il me semble plus judicieux de considérer la conception « éthologique » pour les couches logique et sémantique. C'est ce qu'on peut appeler une *approche hybride de représentation géographique du cyberespace*.

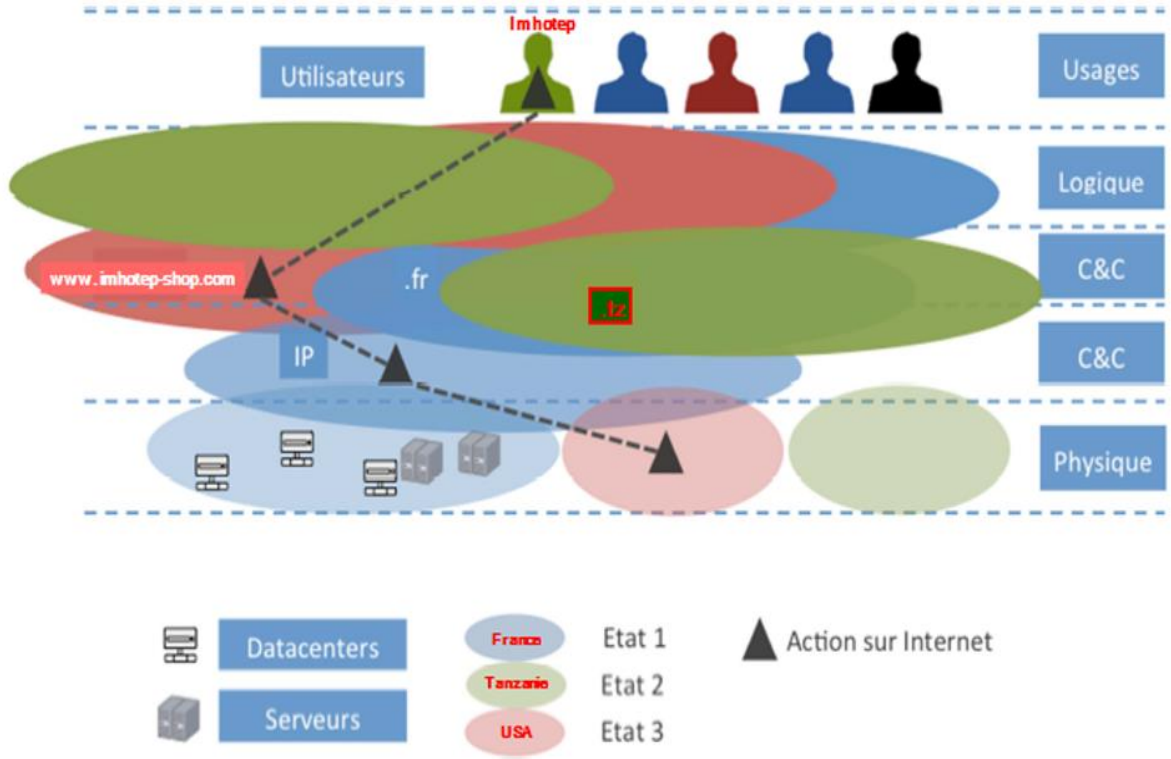
Difficulté de localisation géographique des acteurs dans le cyberespace

Pour illustrer, considérons un jeune *afropreneur*[15] Éthiopien que nous appellerons *Imotep*, opérant dans le secteur agro-industriel en Tanzanie où il vit actuellement. Il commercialise ses produits à partir de sa boutique physiquement localisée en Tanzanie, mais souhaite s'ouvrir au reste du continent pour booster ses ventes. Pour cela, il décide de créer une plateforme en ligne (un site web) afin d'accroitre sa visibilité à l'international. *Imotep* ne fait pas confiance aux prestataires locaux pour héberger son site, et se tourne donc vers un hébergeur situé en France. De plus, *il* a choisi un nom de domaine avec l'extension *dot.com* pour sa plateforme, puisqu'il a toujours entendu dire que c'est le moins coûteux et le plus fiable. Pour être en mesure d'atteindre sa clientèle visée, le jeune éthiopien est contraint de proposer le contenu en plusieurs langue sur sa plateforme (swahili pour la clientèle locale, et anglais pour l'international).

Dans ce contexte, comment situer *Imotep* et sa plateforme dans le cyberespace ? Quel est sa localisation géographique sachant que l'hébergeur est localisé en France (donc soumis au droit et à la souveraineté française), et l'extension de domaine *dot.com* fait partie de l'espace numérique des États-Unis. L'essentiel des clients qui commandent sur la plateforme d'*Imotep* sont eux situés en Afrique de l'Est, visite le contenu en swahili, génèrent et exploitent des données qui sont stockées sur des serveurs en France, potentiellement visible en transit par le gestionnaire de domaine qui est américain. Sachant que le gouvernement tanzanien a légiféré sur le e-commerce et la vente en ligne, à quelle législation est soumise la plateforme de cet afropreneur ? Si le site se faisait piraté, et les données des clients volées, vers qui doit-il se tourner ? Va-t-il traiter différemment les clients locaux et internationaux ? Vous voyez bien la complexité de la chose !

[14] Sébastien-Yves Laurent, *Cyber Strategy : définir un horizon stratégique dans l'environnement cyber*, Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales, 2015

[15] Néologisme pour « entrepreneur africain »



Cas de représentation d'une action pluri-localisée et éparpillée sur plusieurs couches du cyberespace[16]

Dans ce simple scénario pourtant lourd de conséquences en matière de spatialité et de localisation dans le cyberespace, cette approche hybride des conceptions territoriales en rapport avec la structure en couches me semble plus indiquée pour démêler les « juridictions ou les zones de pouvoir » de chaque acteur. Cela permettra aux états africains, pour qui le cyberespace reste pour l'instant un impensé, de mieux graduer leur processus de souveraineté numérique et d'en dégager toutes les conséquences stratégiques (questions de l'anonymat et de la traçabilité des attaquants, de la difficulté d'attribution d'un attaque cyber, de la manière de déterminer qu'une cyberagression est une "attaque armée", de définir le seuil de proportionnalité de la réponse et les règles d'engagement, etc.).

Tant qu'une réflexion sérieuse sur ces aspects n'est pas engagée sur le continent, il sera très difficile pour nos dirigeants de comprendre la cyberguerre (et les moyens qui l'accompagnent) telle qu'elle se déroule aujourd'hui, aussi bien dans nos pays que dans le reste du monde.

[16] Extrait du document cité en note de bas de page 6, légèrement modifié par mes soins pour les besoins de l'exemple.

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, « Comprendre le Cyberespace : un impératif pour l'Afrique ! », Note N°01 - LARC, Mars 2021.