POLICY CENTER FOR THE NEW SOUTH

THINK • STIMULATE • BRIDGE

POLICY PAPER

Décembre 2019

L'Afrique face aux defis proteiformes du cyberespace

Mourad El Manir

PP-19/20

A propos du Policy Center for the New South

Le Policy Center for the New South (PCNS) est un think tank marocain dont la mission est de contribuer à l'amélioration des politiques publiques, aussi bien économiques que sociales et internationales, qui concernent le Maroc et l'Afrique, parties intégrantes du Sud global.

Le PCNS défend le concept d'un « nouveau Sud » ouvert, responsable et entreprenant ; un Sud qui définit ses propres narratifs, ainsi que les cartes mentales autour des bassins de la Méditerranée et de l'Atlantique Sud, dans le cadre d'un rapport décomplexé avec le reste du monde. Le think tank se propose d'accompagner, par ses travaux, l'élaboration des politiques publiques en Afrique, et de donner la parole aux experts du Sud sur les évolutions géopolitiques qui les concernent. Ce positionnement, axé sur le dialogue et les partenariats, consiste à cultiver une expertise et une excellence africaines, à même de contribuer au diagnostic et aux solutions des défis africains.

A ce titre, le PCNS mobilise des chercheurs, publie leurs travaux et capitalise sur un réseau de partenaires de renom, issus de tous les continents. Le PCNS organise tout au long de l'année une série de rencontres de formats et de niveaux différents, dont les plus importantes sont les conférences internationales annuelles « The Atlantic Dialogues » et « African Peace and Security Annual Conference » (APSACO).

Enfin, le think tank développe une communauté de jeunes leaders à travers le programme Atlantic Dialogues Emerging Leaders (ADEL). Cet espace de coopération et de mise en relation d'une nouvelle génération de décideurs et d'entrepreneurs, est déjà fort de plus de 300 membres. Le PCNS contribue ainsi au dialogue intergénérationnel et à l'émergence des leaders de demain.

Policy Center for the New South

Suncity Complex, Building C, Av. Addolb, Albortokal Street, Hay Riad, Rabat, Morocco.
Email : contact@policycenter.ma
Phone : +212 5 37 54 04 04 / Fax : +212 5 37 71 31 54
Website : www.policycenter.ma

POLICY CENTER FOR THE NEW SOUTH

THINK • STIMULATE • BRIDGE

L'Afrique face aux defis proteiformes du cyberespace

Mourad El Manir

L'Afrique face aux defis proteiformes du cyberespace

INTRODUCTION

Le prix du meilleur roman africain de science-fiction au titre de l'année 2017 avait été remporté par Tade Thompson pour son livre intitulé «Rosewater» qui aborde l'histoire d'un agent des services de sécurité luttant contre les cyber-fraudes au Nigéria en 2066. Cette référence à un roman de science-fiction pour introduire les enjeux cybernétiques en Afrique n'est pas fortuite dans la mesure où le mot «cyberespace», inspiré du mot «cybernétique», fut utilisé, pour la première fois, en 1984, par l'auteur de romans de science-fiction William Gibson, pour désigner «Une hallucination consensuelle vécue quotidiennement, dans tous les pays, par des gosses auxquels on enseigne les concepts mathématiques.»

Le rapprochement entre ces deux romans montre que l'Afrique a intégré dans son présent et, surtout, dans son avenir, l'évolution fulgurante des technologies d'information et de communication, qui a généré une véritable transformation de la société et de l'économie mondiales, décrite comme la 4ème révolution industrielle.

Cette révolution dite numérique est actée depuis la fin du 20ème siècle par le développement de l'internet, plateforme mettant en liaison des millions de personnes à travers le monde et, surtout, par une succession de grandes transformations technologiques, portées par la numérisation de données (conversion et stockage d'informations, texte, image, audio…) sous formes de signaux numériques, l'expansion de la connectivité, portée par les réseaux de télécommunication filaire, cellulaire et satellitaire ainsi que l'émergence des techniques d'analyse de données massives ou «Big-data» et par le développement de l'intelligence artificielle. Cette révolution a permis l'émergence d'un nouvel espace de communication et d'échanges avec son corollaire de course à l'influence et au leadership.

Parallèlement et à l'instar de toute activité humaine, l'essor du champ numérique s'est accompagné du développement d'un volet transgressif qui se traduit par l'émergence et le développement de nouvelles menaces aux contours et aux conséquences plus ou moins précis : cybercriminalité, cyber-terrorisme, cyber-conflictualité, posant avec acuité les questions de sécurité des systèmes d'information.

Dans cet environnement aux multiples facettes, l'Afrique, principal centre d'intérêt de cette étude, dont la digitalisation est en nette expansion, tente d'y prendre pied sans être préparée, ni en termes de ressources humaines judicieusement formées, ni sur le registre des infrastructures physiques et informatiques nécessaires. Le continent est également handicapé par le manque d'outils et d'instruments nécessaires pour faire face aux menaces et aux risques générés par le développement du cyberespace et ses conséquences sur la sécurité nationale de ses Etats membres.

L'intérêt de cette étude est de faire ressortir le degré de préparation du continent africain pour faire face aux défis posés par le cyberespace à travers un point de situation sur l'évolution de l'espace numérique. Ceci aussi bien en tant qu'espace conflictuel qu'en

tant que champ d'exercice des relations internationales avant d'examiner la situation cybernétique africaine sous le prisme des avancées enregistrées et des vulnérabilités relevées. La dernière partie sera consacrée aux propositions susceptibles de permettre une meilleure prise en charge des défis cybernétiques par le continent africain.

I. LE CYBERESPACE: UN CHAMP EN PLEINE MUTATION

Espace en pleine expansion, aussi bien sur le plan technologique que sur celui des enjeux induits, le cyberespace s'est érigé en théâtre de conflictualité à part entière et en champ d'expression des relations internationales.

a. Domaine aux contours élargis

Le cyberespace est historiquement lié au réseau de communication américain «Arpanet» (Advanced Research Projects Agency Network), lancé par la Defense Advanced Research Projects Agency (DARPA), relevant du Département de la Défense des Etats-Unis, à la fin des années 1960, pour assurer la survie du système de transmission de l'armée américaine en cas d'attaque nucléaire massive soviétique. Pour un usage civil, l'Arpanet deviendra Internet avec la création des noms de domaines en 1983 et du world wide web (www.) en 1989.

Souvent confondu avec Internet, la définition du cyberespace est extensible. Elle est établie en fonction des intérêts stratégiques de chaque acteur qui y évolue. En effet, elle est, à l'instar de la définition de tout nouveau concept, sujette à polémiques et à des interprétations diverses. Ainsi, le cyberespace est désigné, tantôt comme un environnement, un domaine, un milieu ou un moyen, tantôt comme un théâtre d'opérations, un espace ou un substrat.[1]

Dans tous les cas, il n'est pas perçu comme un bloc homogène et uniforme, mais comme un domaine dans lequel chaque acteur, chaque usager, construisent leur propre conception en fonction de leurs intérêts ainsi que de leur perception des risques et des menaces.

Ce faisant, la littérature sur la définition du cyberespace est foisonnante. Le petit Robert décrit le cyberespace comme «un ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs», tandis que dans son rapport «Défense et Sécurité des Systèmes d'information. Stratégie de la France», publié en 2011, l'Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI, décrit le cyberespace comme «l'espace de communication constitué de l'interconnexion mondiale d'infrastructures et d'équipements de traitement automatisé des données numérisées.» [2]

Les chercheurs se sont également penchés sur la question. Dans leur ouvrage «cyberwar», Richard Clarke et Robert Knake définissent le cyberespace comme «l'ensemble des réseaux informatiques mondiaux et tout ce qu'ils connectent et permettent de contrôler.

1. Alix Desforges : les représentations du cyberespace : un outil géopolitique. Hérodote 2014.
2. Cette définition est celle publiée dans le rapport de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), français, en 2011, dénommé «Défense et sécurité des systèmes d'information. Stratégie de la France.» Disponible sur le site : www.ssi.gouv.fr. Cette approche est souvent critiquée, du fait qu'elle limite la définition du cyberespace à sa seule définition technique, occultant ses autres aspects, notamment la dimension stratégique incluant tous les échanges et activités d'ordre social, économique, sécuritaire ou juridique, rendus possibles par Internet

Il ne s'agit pas seulement de l'internet, mais de tous les autres réseaux informatiques qui ne sont pas censés être directement accessibles depuis Internet.»[3]

En revanche, Athina Karatzogianni a souligné, dans un livre consacré à ce sujet, que la cyber-conflictualité qui représente les conflits par ordinateur dans des environnements médiatisés, englobe deux tendances : le cyber-conflit ethno-religieux opposant des groupes ethniques ou des groupes religieux dans le cyberespace (Kosovo) et le cyber-conflit sociopolitique entre un mouvement social et son institution antagoniste (mouvement antimondialisation).[4]

Pour tenter de réduire le gap entre les appréciations, des experts américains et russes ont proposé une formulation se voulant consensuelle, définissant le cyberespace comme «un support électronique par lequel l'information est créée, transmise, reçue, stockée, traitée et supprimée.»[5]

Il reste qu'englobant aussi bien des aspects matériels qu'immatériels, le cyberespace ne peut être conçu qu'à travers la sédimentation de trois couches,[6] qui s'articule autour de:

- La couche matérielle, composée d'infrastructures matérielles. Elle constitue la partie physique d'Internet, avec ses serveurs, ses câbles sous-marins, ses Datacenter, les réseaux de téléphonie mobile, les fibres optiques terrestres, etc. Cette couche dépend des législations nationales. Les installations sont jugées d'importance vitale et font l'objet de mesures particulières de sécurité.
- La couche logicielle, qui englobe l'ensemble des programmes et applications permettant d'accéder au réseau, d'effectuer des requêtes, d'obtenir des services et d'assurer le transport des données. La sécurisation de cette couche est au centre d'enjeux cruciaux, compte tenu des préjudices financiers qui peuvent en découler ;
- La couche cognitive qui se rapporte au contenu informationnel, véhiculée sur les pages d'internet. Cette couche constitue l'espace où se mêlent les perceptions de la réalité et les capacités de la gestion de la connaissance. Les vulnérabilités inhérentes à cette couche portent sur la désinformation, les fake news, l'usurpation d'identité ou les atteintes à la réputation en ligne.

La dimension élargie du cyberespace se traduit surtout par le nombre des acteurs qui y évoluent. En effet, les Etats qui ont fait de l'espace numérique une priorité de leurs stratégies de sécurité nationale, en s'efforçant d'encadrer les activités cybernétiques se déroulant sur leur territoire et en tentant d'influencer les activités dans leur zone d'influence ou d'intérêt, se voient concurrencer dans leur monopole de l'usage légitime de la force physique par d'autres acteurs qui y opèrent avec des enjeux et des objectifs différenciés.

Dans ce cadre, les organisations internationales, conscientes des enjeux portés par le cyberespace, tentent de s'y assurer des espaces d'intervention et de compétence. Les superpuissances économiques tout autant que les opérateurs privés (comme l'ensemble GAFAM : Google, Apple, Facebook, Amazon, Microsoft) tentent de contrôler les flux de

3. Richard Clarke et Robert Knake, «cyberwar», harper collins publishers, 2010
4. Athina Karatzogianni, «The politics of cyberconflict». Edition Routledge. Septembre 2006.
5. Russia-US bilateral on cybersecurity, Critical Terminology foundations, Avril 2011, consultable sur :www.ewi.info/cybersecurity-terminology-foundations.
6. La théorie des trois couches du cyberespace a été développée, par Daniel Ventre, dans son livre «Cyberespace et acteurs du cyber-conflit». Editions Lavoisier. 2011.

données qui y circulent pour s'assurer une posture hégémonique, notamment dans le domaine commercial. Des collectifs (organisations non gouvernementales, groupe d'influence) sont en mesure d'infléchir le cours des événements et toute une gamme d'acteurs individuels (hackers, cybercriminels) s'y livre à des activités illicites.

Il y a lieu de préciser que toute nuisance portée dans le cyberespace est considérée comme une cyber-attaque, dont l'enjeu reste le contrôle de l'information, sous différentes facettes :

- l'information diffusée à des fins de propagande (médiatisation de fake-news) ;
- l'information recherchée pour acquérir des connaissances (secrets, brevets ou données) ;
- l'information protégée en vue de sauvegarder ses propres donnés.

Ce faisant, la cyber-sécurité est définie comme «l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles. La cyber-sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyber-défense.»[7]

Dans ce cadre, la cybercriminalité correspond à «l'ensemble des crimes et délits traditionnels ou nouveaux réalisés via les réseaux informatiques.» En revanche, la cyber-défense traduit «l'ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces de sécurité, la réalisation des missions confiées et le bon fonctionnement des institutions»[8].

En plus de ces deux concepts, le développement du cyberespace a généré d'autres menaces comme le cyber-terrorisme appréhendé comme l'utilisation d'internet dans les conflits asymétriques opposant des parties n'ayant nécessairement pas la même nature juridique (il peut s'agir d'un Etat, d'une entreprise, d'un collectif de militants ou d'un individu isolé.)

Le tableau joint en annexe fait ressortir le type de cyber-nuisances en fonction des interactions des différents acteurs.

b. Une conflictualité consacrée

L'évolution du champ cyber et ses conséquences sur les activités humaines, de plus en plus dépendantes des technologies d'information et de communication, a conduit au développement d'une conflictualité qui, elle-même, a généré la mise en place de capacités cybernétiques.

Ainsi, depuis la cyber-attaque contre l'Estonie en 2007, le cyberespace est considéré comme un théâtre d'opération au même titre que les milieux aéroterrestre et maritime.

La conflictualité dans ce milieu n'est pas perçue comme un affrontement de technologies, mais comme «l'utilisation des moyens numériques à des fins de contrôle de

7. ANSSI, Défense et Sécurité des Systèmes d'information. Stratégie de la France, Février 2011.www.ssi.gouv.fr.
8. Définition du Ministère français des Armées. www.defense.gouv.fr

la volonté de l'adversaire», rejoignant, en cela, la célèbre formule du théoricien allemand Carl Von Clausewitz «la guerre n'est que le prolongement de la politique par d'autres moyens».

Dans ce cadre, la conflictualité du cyberespace est mesurée à l'aune des cyber-attaques intervenues dans le champ des affrontements globaux qui s'inscrivent dans le cadre des tensions géopolitiques mondiales. (Tableau détaillé des cyber-attaques en Annexe).

Ainsi, la détermination russe d'empêcher toute réduction de sa sphère d'influence est souvent avancée pour expliquer les cyber-attaques intervenues dans l'ex-espace soviétique:

- En 2007, l'Estonie fut la cible d'une opération de déni de service causant la paralysie des services en ligne de son administration et l'interruption des transactions par Internet de ses banques. Cette attaque est survenue sur fond de tension avec la Russie au sujet du projet de déplacement d'un monument rendant hommage aux soldats soviétiques (le soldat de bronze).[9]
- En 2008, en Géorgie, des réseaux informatiques ont été piratés et des graffitis sont apparus sur les sites gouvernementaux, au moment où le pays était en conflit avec la Russie. [10]
- En 2014, en Ukraine, un virus dénommé «Snake» a infiltré les ordinateurs du Premier ministre ukrainien et une dizaine d'ambassadeurs ukrainiens en Europe. Des informations sensibles auraient été dérobées. L'origine russe de ces cyber-attaques est fortement supposée. [11]

De même, des cyber-attaques sont menées dans le cadre des tensions géopolitiques pour pallier le recours à des affrontements traditionnels, dont les conséquences seraient lourdes.

Il en est ainsi pour l'opération «olympic Games», médiatisée en octobre 2010, qui a porté sur l'implémentation d'un virus informatique «Stuxnet» dans les systèmes de contrôle des centrifugeuses d'enrichissement d'uranium de la centrale iranienne de Natanz, en vue de ralentir le projet nucléaire iranien[12]. La même dynamique anime les cyber-attaques ponctuant les relations sino-américaines ou les crises récurrentes avec la Corée du Nord.

La conflictualité du cyberespace est consacrée aussi par l'institutionnalisation de capacités cybernétiques, à travers la mise en place d'une force de frappe cybernétique, comprenant un commandement et des forces dédiés aux opérations, des stratégies et des tactiques adaptées ainsi que des ressources matérielles, humaines et financières.

Pour ne prendre que l'Exemple des Etats-Unis, ce pays qui s'est doté d'un commandement dédié à la cyber défense (US Cybercom en 2010), de budgets conséquents (50 milliards de dollars de 2010 à 2015,), de stratégies liées au cyberespace (Startegic for operating in cyberespace en 2011 et «the DOD cyberstrategy» en 2015), des ressources humaines qualifiées (plus de 3000 hommes), organise, annuellement, des exercices et des simulations liés au domaine cybernétique (cyberstrom).[13]

9. Les cyber-attaques. Repères chronologiques-NATO, consultable sur le site : www.nato.int.doc.timeline.
10. Les cyber-attaques. Repères chronologiques-NATO, consultable sur le site : www.nato.int.doc.timeline.
11. Observatoire du monde cybernétique. Lettre n°32-aout 2014. Page 2, consultable sur le site: www.defense.gouv.fr
12. Jacques Benillouche « comment le virus Stuxnet s'en est pris au programme nucléaire iranien», article consultable sur le site: www.slate.fr
13. Dans une conférence animée par la Ministre des Armées françaises Florence Parly, le 18 janvier 2019, elle a précisé que «le projet cybernétique français qui prévoit une armée cyber de 4000 hommes à l'horizon de 2025 projette de consacrer un budget de 1,6 milliard d'euros à ce secteur». Déclaration reprise par plusieurs médias, notamment «BFMTV», sous le titre «comment la France se prépare à une cyber-guerre mondiale»

En plus des Etats, les organisations de sécurité collective internationale ont acté la conflictualité du cyberespace. Ainsi, en 2016, à l'issue du Sommet, tenu à Varsovie en Pologne, l'OTAN a désigné le cyberespace «terrain des opérations militaires» et s'est investie dans les efforts visant à sa réglementation.

A ce titre, après le premier guide de cadrage juridique international des problématiques conflictuelles cybernétiques, appelé, «Manuel de Tallinn», publié en 2013, l'Alliance atlantique a chargé un panel d'experts d'approfondir cette question. Travail qui a abouti à la publication d'un deuxième ouvrage en 2017.

Il y a lieu de préciser que la question de régulation de l'espace cybernétique reste au centre des préoccupations internationales. Le premier traité, dit «Convention de Budapest», qui porte sur la cybercriminalité, a abordé les crimes informatiques et les crimes sur internet, y compris la pornographie infantile, l'atteinte au droit d'auteur et le discours de haine en harmonisant certaines lois internationales. Entrée en vigueur en 2007, cette Convention compte 64 Etats membres et 09 pays en tant qu'observateurs.[14]

En 2013, les Etats, réunis au sein du Groupe des Experts Gouvernementaux (CGE), chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale au sein des Nations unies, ont affirmé que le droit international et, en particulier, la charte des Nations unies, sont applicables au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible.

Cependant, les réponses, en droit international, offertes à un Etat victime d'une cyber-opération sont confrontées à la difficulté d'attribuer l'attaque à un autre Etat. L'Etat cible est également confronté au rôle important des acteurs privés dans le cyberespace.

Il reste que le droit international permet aux Etats, grâce à l'obligation de diligence «due diligence», d'engager la responsabilité internationale d'un Etat à partir du territoire duquel une cyber-opération, portant atteinte aux droits de l'Etat victime, a été lancée.

Dans ce registre, les interrogations portent également sur l'applicabilité du droit de la guerre dans ce nouveau théâtre des opérations, notamment l'attribution des attaques, le seuil et les formes de la légitime défense, la compatibilité des actions offensives avec les principes du droit international humanitaire, etc.

A titre d'exemple, bien que la Russie soit fortement soupçonnée d'être l'instigatrice des cyber-attaques en Estonie, en Géorgie et en Ukraine, aucune accusation formelle n'a été émise contre ce pays.

c. Champ établi des relations internationales

Les relations internationales sont régies, depuis le 24 octobre 1648, par les traités de Westphalie, basées sur l'Etat Nation comme socle du droit international.

Cependant, avec l'émergence de nouveaux acteurs dans le cyberespace (groupes privés ainsi que des acteurs individuels et collectifs), la place centrale de l'Etat dans le champ des relations internationales

14. Site web du Conseil de l'Europe : www.coe.int.

se trouve perturbée, notamment par rapport aux dimensions de souveraineté internationale.

Dans ce cadre, le concept de Puissance, l'un des sujets de prédilection de l'étude des relations internationales et principal critère de l'appréciation de la politique internationale, se trouve relativisé, reconfiguré ou contourné. Joseph Nye qui définit la puissance comme «la capacité d'influence pour obtenir des résultats attendus par l'utilisation du Hard power (la coercition et les amendes) et du soft Power (influencer l'agenda politique, exercer une attraction et une persuasion)[15], souligne que le cyberespace a abaissé le seuil d'accès[16] à l'arène internationale, compte tenu qu'il suffit d'un ordinateur et d'une connexion internet, sans même avoir besoin d'être un expert en sécurité informatique, pour mener une cyber-attaque.

La dissuasion est un autre concept des relations internationales affecté par la cyber-conflictualité. En effet, les Etats, particulièrement les Puissances, cherchent le moyen de dissuader leur adversaire d'attaquer leurs infrastructures.

Dans ce registre, l'administration américaine, sous Barack Obama, consciente des difficultés de l'application d'une cyber-dissuasion dans le cyberespace a adopté une stratégie de dissuasion globale qui se manifeste par une escalade dans la rhétorique stratégique. Cette posture, expliquée dans l'»International Strategy For Cyberespace», précise que si les Etats-Unis sont attaqués par une cyber-attaque de grande ampleur, ils se réservent le droit d'utiliser tous les moyens pour protéger leurs intérêts.[17]

Par ailleurs, le cyberespace ébranle la notion de souveraineté. En effet, la question de souveraineté numérique, dans le sens de la capacité des Etats à contrôler les flux et à exercer leur autorité sur ceux qui les produisent, ceux qui les transpostent et ceux qui les reçoivent, est difficilement applicable sur la scène westphalienne dans laquelle la souveraineté est intimement liée à la notion de territoire.

Pour mieux appréhender cet enjeu de souveraineté et contrôler le cyberspace et les données qui y circulent, les Etats ont lancé d'importants programmes de cyber-sécurité et de cyber-défense. Ces processus d'appropriation du cyberespace et des données ont engendré des rapports de rivalité et de pouvoir, mettant en jeu des acteurs très inégaux.

Dans ce registre, la question des Data-center est édifiante. En effet, le contrôle des données est devenu un problème de sécurité pour les Etats (données stratégiques) comme pour les populations (données personnelles). Ce contrôle passe d'abord par l'acquisition et le développement d'infrastructures nationales de stockage de données sensibles et par leur maintien sur le territoire national.

De même, l'espace numérique agit sur la perception des enjeux sécuritaires, dans le sens de l'articulation et de l'usage des outils techniques, que ce soit en matière de surveillance, d'anticipation ou de détournement des contenus numériques. Dans ce cadre,

15. Joseph S. Nye «Power and national security in cyberespace» in America's cyber future, Security and Prosperity in the information Age. Juin 2011.
16. On appelle seuil d'accès, les conditions pré-requises pour devenir un acteur à part entière.
17. Dans un entretien accordé au journal français «le Journal du Dimanche», le 08 janvier 2017, l'ex-ministre français de la défense avait précisé que « face à une cyber-attaque, la France peut riposter par tous les moyens»

les questions des Big-data et des intelligences artificielles ne relèvent pas uniquement des solutions techniques mais s'inscrivent dans des logiques sécuritaires. En effet, les Big-data jouent un rôle important dans la gestion de l'information à l'ère numérique. Du point de vue des algorithmes, les données massives facilitent certaines activités dans le domaine de la recherche de l'information.

Enfin, la numérisation modifie les rapports de force sur la scène internationale. Dans ce cadre, le leadership des Etats-Unis dans le domaine numérique est sans précédent.

Cette suprématie américaine sur Internet est, aujourd'hui, évidente, à tous les niveaux, que ce soit pour les infrastructures physiques, les avancées techniques, la recherche technologique, le poids économique ou l'influence réglementaire[18]. Ce faisant, cette position dominante permet aux Etats-Unis de peser sur trois domaines, appelés à influer sur l'avenir du cyberespace : la stabilité économique, la sécurité internationale et la réglementation dans l'espace numérique.

II. LE CYBERESPACE AFRICAIN: UN CHAMP AUX CONTRADICTIONS MANIFESTES

Le cyberespace est passé, incontestablement, du registre technique à celui de domaine aux enjeux multiples, à l'origine de cyber-conflits et de rivalités internationales. Dans ce cadre, l'Afrique qui semble avoir réussi à négocier, relativement, le tournant technique, n'est pas en mesure de se positionner sur le registre conflictuel, encore moins diplomatique.

a. Des avancées indéniables

La rentrée de l'Afrique dans l'ère numérique est une réalité incontestable. En effet, sur les trois indicateurs adoptés à l'échelle internationale, les chiffres réalisés par le continent sont prometteurs. Ainsi, en à peine quelques années, le taux d'accès de la population à Internet a enregistré une avancée exponentielle. Au 30 juin 2019, ce taux atteignait 39,8% alors qu'il n'était que de 5% en 2007[19], la moyenne mondiale étant de 57,3%. D'après le cabinet Deloitte, l'Afrique compte aujourd'hui 450 millions d'Africains connectés (sur 1,2 milliard) via leur Smartphone. Sur le nombre d'utilisateurs actifs de Facebook, l'Afrique se prévaut de 211 millions (janvier 2019), soit une progression de 15% par rapport à 2018. La région la plus connectée reste l'Afrique du Nord. Enfin, sur le taux de pénétration de la téléphonie mobile, qui constitue la porte d'entrée de l'Afrique dans le monde digital, le continent comptera 660 millions équipés d'un Smartphone en 2020, soit le double qu'en 2016.

En termes d'avancées, il y a lieu de souligner aussi le développement d'une économie numérique, notamment dans les secteurs bancaires (l'Afrique est bien positionnée dans le registre de «mobile banking»), les services en ligne, les télécommunications, les médias, les assurances mais aussi dans les secteurs de l'éducation et de la culture ou encore de la santé. Dans ce cadre, les revenus issus de la téléphonie mobile représentent 3,7% du PIB sur le continent africain, soit le triple de ceux des économies développées.

18. Stéphane Taillat, Amael Cattaruzza, Didier Danet. «la Cyberdéfense, politique de l'espace numérique» Editions Armand Colin. 2018.
19. www.internetworldstats.com

Même dans le domaine de l'intelligence artificielle, le continent est en passe de conquérir une part de ce marché d'avenir. En juin 2018, l'entreprise américaine Google a annoncé l'ouverture d'un centre de recherche en intelligence artificielle au Ghana pour inclure cette technologie dans les programmes de formation et de développement. Le spécialiste américain du Big Data, l'entreprise SAS, a annoncé l'investissement d'un milliard de dollars en Afrique pour financer la formation des ressources humaines et l'accès des opérateurs locaux aux dernières technologies liées à l'intelligence artificielle.

Dans ce cadre, le Togo accueillera du 16 au 17 décembre 2019, un symposium régional sur le thème : «Pour une intelligence artificielle (IA) éthique et inclusive au service du développement durable, de la paix et de la sécurité en Afrique de l'Ouest», en marge duquel sera posée la première pierre de l'Agence francophone de l'intelligence artificielle (Afria) à Aneho.[20] Ce symposium intervient après le 1er forum africain sur l'intelligence artificielle organisé par l'Unesco en décembre 2018 à l'université polytechnique de Ben-Guerrir au Royaume du Maroc.

Par ailleurs, certains pays africains ont entamé des évolutions substantielles dans des secteurs très pointus comme celui de la Block-Chain.[21]. L'Afrique du Sud a mis sur pied la «Blockchain Academy» qui offre des formations sur les crypto-monnaies et la technologie de Blockchain. Le Kenya a mis sur pied un groupe de travail sur cette technologie en particulier et sur l'intelligence artificielle comme moyen d'optimiser la gestion publique. Au Nigéria, des organisations se multiplient pour la maitrise de l'environnement des monnaies numériques. En Ouganda, le gouvernement est fortement impliqué dans l'introduction de la Block-Chain dans le secteur bancaire en vue de réduire les coûts opérationnels et les risques. La sierra Leone se prévaut de l'utilisation de la Block-Chain dans la gestion des processus électoraux.

Sur le plan des législations, les gouvernements africains mettent progressivement en place des mesures sous forme de lois, d'organisations spécialisées et d'infrastructures pouvant assurer la protection numérique du grand public (entreprises et citoyens). En plus du volet juridique, plusieurs Etats africains ont mis en place des autorités nationales compétentes en la matière ainsi que des équipes opérationnelles de réponses immédiates.

Dans un rapport sur les évolutions en cyber-sécurité, rendu public en 2017, l'Union internationale des télécommunications (UIT) a précisé que plusieurs pays africains ont mis en place de bonnes pratiques de renforcement des capacités de lutte contre la cybercriminalité

La question cybernétique est également prise en charge par certaines organisations régionales. La Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO) a mis en place une initiative régionale qui organise régulièrement des forums sur des sujets relatifs à la cyber sécurité et la Communauté de développement de l'Afrique Australe (SADC) coordonne les efforts de ses Etats membres pour renforcer la cyber-sécurité en Afrique australe.

Sur le plan continental, l'Union africaine a adopté «la convention sur la cyber sécurité et la protection des données à caractère personnel «, à l'issue de la 23ème

20. Marie –France Réveillard «la première agence pour l'intelligence artificielle en Afrique francophone siégera au Togo». La tribune. fr, le 12 septembre 2019.
21. Block-Chain peut être défini comme la technologie de stockage et de transmission d'information, transparente, sécurisée et fonctionnant sans organe central. C'est une sorte de base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création en 2008.

Assemblée des chefs d'Etat et de gouvernement de l'Union africaine, tenue à Malabo les 26 et 27 juin 2014. Cette convention appelée «Convention de Malabo» a pour but de mettre en place un cadre juridique pour la cyber sécurité et la protection des données personnelles.

Compte tenu de l'importance de cette question, l'UA a inscrit la cyber-sécurité en tant que programme phare de l'Agenda 2063, traduisant le souci d'incorporer dans les plans africains de développement, les changements provoqués par les technologies émergentes, en veillant à ce qu'elles soient utilisées par les particuliers, les institutions et les Etats dans de bonnes conditions de sécurité.

Sur le plan opérationnel, l'Africa-CERT, lancé le 30 mai 2010 à Kigali au Rwanda, vise à aider les pays africains à créer et à mettre en place des équipes de sécurité informatique et d'intervention en cas d'incident. Il y a lieu de préciser que les pays africains membres de l'Organisation de la Conférence islamique (OCI) bénéficient de l'expertise de «l'OIC- CERT»

Dans le domaine de la cyber-défense, les acquis, bien que modestes, ont le mérite d'exister. Ils sont encadrés par des initiatives privées. Les pays de l'Afrique australe organisent, de manière bisannuelle, un forum portant le nom «Africa Cyber Defence Summit».[22]

Par ailleurs, des études sont menées, actuellement, pour procéder à l'ouverture de trois centres d'opérations de cyber-défense, au Nigéria, à l'Ile Maurice et au Sénégal, en plus de celui déjà ouvert en Afrique du Sud.

Il reste que si les avancées cybernétiques africaines sont une réalité tangible, les vulnérabilités ne le sont pas moins.

b. Des vulnérabilités persistantes

Sur le plan technologique, le continent enregistre une inégalité dans l'accès à l'espace numérique. En effet, certaines régions et une grande partie de la population sont totalement absentes du cyberespace, de ses enjeux et de ses retombées économiques. Cette situation est due à la faiblesse des infrastructures nationales, rendant une connexion à internet onéreuse : en République centrafricaine ou en Guinée, une connexion haut débit peut couter jusqu'à 500 dollars par mois.

Dans le même registre, l'Afrique connaît une fissure cybernétique entre les Etats[23] ayant massivement investi dans le cyber (infrastructures, concepts d'emploi, moyens) quand d'autres manquent de ressources nécessaires pour assurer une protection minimum.

Cette déficience a été mise en évidence par une enquête de la Commission de l'Union africaine sur les tendances de la cyber sécurité et de la cybercriminalité en Afrique qui a souligné que seulement 15 pays africains ont mis en place une législation en matière de cybercriminalité.

Ces conclusions ont été largement réitérées lors de l' «AfricaSEC 2019», tenue à Marrakech, les 8 et 9 février 2019, qui a relevé que les Etats africains sont divisés entre trois tendances : La majorité n'a

22. Francois-Xavier Djimgou «Souveraineté numérique et cyber-défense : un enjeu de taille pour l'Afrique». Editions Edilivre. 2019.
23. Au sein même des Etats africains, la fissure cybernétique existe entre les zones urbaines et les zones rurales.

entrepris aucune démarche alors qu'une minorité a mis en place des mesures concrètes, tandis qu'au milieu, un groupe d'Etats a adopté des instruments juridiques sans actions concrètes.

En termes de cyber-nuisance, l'Afrique remporte la palme de la cybercriminalité. Cette situation ne cesse d'être dénoncée[24]. Elle est induite par l'accessibilité d'internet, le développement de la 3G/4G, l'anonymat sur le web, le manque de sécurisation de certaines infrastructures critiques et sensibles ainsi que par le manque de sensibilisation des acteurs évoluant dans les entreprises et des populations à la cyber-sécurité.

Dans ce registre, le panorama cybercriminel-istique africain est particulier. Il inclut le piratage des serveurs téléphoniques, communément appelé «phreaking», le piratage des systèmes d'informatiques avec demande de rançon «ransomware», la manipulation du trafic d'un site internet avec le but de dérober des informations confidentielles, le «pahrming» ainsi que la cyber escroquerie dans ses différentes formes, allant de l'arnaque aux sentiments au chantage à la vidéo, en passant par les faux visas ainsi que les fausses offres d'emploi et de bourses d'études.

La cybercriminalité ciblant les entreprises englobe les atteintes aux systèmes de traitement automatisé de données, les violations de données personnelles, les atteintes à l'e-réputation, ainsi que la contrefaçon de marques et de logiciels.

Cette cybercriminalité africaine à un coût. Il est énorme. En effet, la société de cyber-sécurité kenyane Serianu qui a diligenté un audit en partenariat avec plus de 700 institutions publiques et privées africaines, fait état de chiffres alarmants.

Rien que pour l'année 2017, la cybercriminalité continentale a engendré des préjudices financiers considérables : le Nigéria (649 millions de dollars) le Kenya (210 millions de dollars) ou encore la Tanzanie (99 millions de dollars). Au total, le continent a enregistré une perte de 3,5 milliards de dollars pour l'année 2017.

D'un autre côté, le continent enregistre une déficience criante en matière de cyber-défense. L'incident le plus significatif porte sur les révélations de l'espionnage du siège de l'Union africaine par la Chine de janvier 2012 à janvier 2017.

L'affaire, rapportée par la presse mondiale, fait état que des dispositifs chinois mis en place lors de la construction du siège de l'Union Africaine, par des entreprises chinoises avec des systèmes informatiques livrés clés en main, permettaient de transférer chaque nuit, l'intégralité du contenu des serveurs du bâtiment de l'organisation africaine vers des ordinateurs situés à Shanghai. L'Etat chinois aurait eu accès, non seulement à l'ensemble des documents produits par l'organisation, mais également aux lignes téléphoniques et aux micros des visioconférences, installés sur le site.

Le leadership africain est également ciblé par d'autres pays comme l'a mis en évidence le journal français «le Monde» qui avait publié une enquête sur les plateformes occidentales de recherche des informations sur les hauts cadres africains.[25]

24. Lors du «4ème Africa Cybersecurity Conference d'Abidjan», tenue les 3 et 4 octobre 2019, les intervenants ont déploré que «l'Afrique reste le continent le plus exposé à la cybercriminalité»
25. Journal «le Monde», intitulé «Chefs d'Etat, diplomates, hommes d'affaires, le Who'Who des écoutes britanniques en Afrique.» Publié, le 08 décembre 2016.

Sur la question du cyber-terrorisme, dans le sens de l'utilisation réseaux sociaux pour véhiculer des messages de haine, le recrutement de djihadistes ou la collecte de financements occultes, les experts restent sceptiques sur le concept, en avançant que dans beaucoup de pays africains, touchés de plein fouet par le terrorisme (Nigéria, Niger, Tchad, Soudan, Ethiopie, Somalie) le taux d'abonnement au téléphone mobile est inférieur aux moyennes africaines.

Dans son livre «l'Afrique, nouvelle frontière du Djihad», Marc-Antoine Pérouse de Montclos précise que « des sondages réalisés auprès d'anciens combattants de Boko Haram dans des camps déplacés au Nigéria ont montré qu'aucun d'entre eux n'a été recruté en ligne»[26]

Concernant les enjeux internationaux liés au numérique, l'Afrique enregistre un retard considérable sur la question stratégique des Datacenter, dans le sens d'infrastructures de stockage et de traitement de données. L'enjeu est de maintenir les données stratégiques et les données personnelles sur le sol africain.

Actuellement, le continent ne compte que 80 Centres de Données dont la moitié est implantée en Afrique du Sud. La situation est telle qu'une importante part des données africaines est stockée et exploitée en dehors du continent. Sur ce sujet, une importante bataille est engagée sur la future mise en place des Datacenter africains, dans laquelle les pays anglophones, particulièrement ceux ayant un accès à la mer (proximité des câbles marins) ont la prééminence. Il y a lieu de signaler que le Royaume du Maroc est en passe de se positionner comme un hub pour les Datacenter au Nord de l'Afrique.

Par ailleurs, le besoin africain en investissements et en transfert de technologies dans le domaine cybernétique place l'Afrique dans une posture de vulnérabilité extrême, à tel point que des experts n'hésitent pas à parler de «cyber-colonialisme».

Ce concept est défini comme «la politique ou la pratique permettant de prendre le contrôle total ou partiel du cyberespace d'un pays, par des technologies et de l'exploiter économiquement». Le doigt accusateur est dirigé vers les Gafam qui, en offrant des services gratuits (Facebook), organisent le secteur du numérique en Afrique pour pouvoir le contrôler à leur profit. L'ONG Global Justice Now a publié, en mai 2018, un rapport, au titre évocateur : «Comment l'agenda global du e-commerce annonce le pouvoir des grandes firmes numériques et menace le Sud.»

En dernier lieu, le continent africain est confronté au développement considérable des pratiques de manipulation des informations (Fake news), induit par la facilité d'accès à l'Internet et aux Smartphones ainsi qu'au faible taux de sensibilisation des populations. La situation est telle que les «fake news» sont considérées comme une menace à la paix sociale sur le continent, particulièrement[27] en Afrique subsaharienne.

En effet, récemment, la diffusion de fake news a potentiellement :

- déclenché des violences ethniques à cause de photos manipulées de corps de Somaliens de souche poussés dans une tombe peu profonde dans la région d'Oromia en Ethiopie ;
- semé la confusion parmi les électeurs du scrutin présidentiel du Nigéria, suite à de fausses

26. Marc-Antoine Pérouse de Montclos, «l'Afrique, nouvelle frontière du djihad», éditions la découverte. 2018
27. Ecofin hebdo, «l'explosion des fake news en Afrique, une menace pour la paix sociale et la pérennité des réseaux sociaux.» Article publié le 14 février 2019.

informations sur les candidats ;
- provoqué des fluctuations monétaires après la rumeur de la démission du président sud-africain Jacob Zuma.

En tout état de cause, les vulnérabilités cybernétiques africaines, réelles, nécessitent la mise en place d'actions concertées visant à consolider les acquis et à réduire les déficiences.

c. Consolidation des acquis et réduction des déficiences

Compte tenu des enjeux cybernétiques en présence, la mise en place d'une cyber-stratégie africaine, une impérieuse nécessité passe par l'instauration d'un climat de confiance. En effet, l'espace cyber est un domaine où la méfiance est de rigueur, compte tenu des révélations sur les écoutes et les activités de surveillance auxquelles se livrent les Etats entre eux, en utilisant justement les moyens offerts par le cyber.

Par ailleurs, le continent africain, doit partir en rangs unis pour consolider sa digitalisation, en vue de disposer de l'outil qui lui permettra, le cas échéant, de se positionner en acteur efficace et efficient dans l'espace numérique. Dans ce cadre, il doit relever, dans l'immédiat, trois défis :

- la connectivité : bien que le niveau de la connectivité du continent africain est en nette progression, il demeure en deçà des chiffres mondiaux. Dans ce cadre, il y a lieu de renforcer les infrastructures des pays africains de manière à rendre la connexion à internet moins onéreuse.
- l'infrastructure électrique : une attention particulière doit être accordée à la résolution des problèmes d'approvisionnement et de délestage électrique, avant d'investir dans les infrastructures nationales des technologies de l'information et de communication.
- les équipements : la numérisation du continent est tributaire de la réalisation des équipements adéquats. Outre leur réalisation, les Etats africains doivent s'approprier la capacité de leur utilisation. Par ailleurs, ils doivent encourager la mutualisation des moyens, pour réaliser des économies d'échelle.

En termes de cyber-menaces, la lutte contre la cybercriminalité doit être placée en première priorité, en axant l'effort sur la formation et la sensibilisation :

- la formation des spécialistes qui doit englober la formation initiale pour constituer un vivier de professionnels de la sécurité. Elle doit, aussi, englober la formation continue en vue de renforcer l'expertise des acteurs sur le terrain ;
- la sensibilisation à la sécurité de l'ensemble des filières des autres corps de métier de l'informatique, ingénieurs systèmes et réseaux, développeurs, ainsi que tous les citoyens de façon globale, plus particulièrement aux techniques d'ingénierie sociale. Dans le cyber-domaine, chaque utilisateur est un membre actif de la chaine de cyber-sécurité et une chaine n'est jamais solide que par son maillon le plus faible.

La lutte contre la cybercriminalité doit englober, aussi, des actions opérationnelles portant :

- généralisation des capacités de réaction. A cet effet, les structures de type CERT (Computer emergency response team), doivent être généralisées à l'ensemble des pays africains. Bien plus,

la mise en place d'un centre africain de cyber-opérations comme lieu d'intégration des capacités nationales, est de nature à renforcer la résilience cybernétique.

- mise à niveau juridique, en apportant un soutien aux pays africains trouvant une difficulté à mettre en place une législation adaptée aux défis cybernétiques. Dans ce domaine, les mécanismes juridiques mis en place doivent accompagner le développement de la technologie et des cyber-nuisances.

Sur le plan de la cyber-défense, talon d'Achille de la cybernétique africaine, l'action doit privilégier, de prime abord, la coopération intra-africaine, susceptible d'harmoniser les efforts.

Ce panafricanisme cybernétique passerait par :

- la mise en place d'une structure africaine de cyber-défense, rattachée à l'Union africaine qui pourra être constituée de représentants des Etats membres mais aussi d'experts de la société civile et du secteur privé africain. Cette structure aura pour mission d'élaborer une vision africaine de la souveraineté numérique ;
- l'amélioration de la protection des réseaux de communication existants ;
- la facilitation des échanges entre les Etats membres des doctrines en matière de cyber- défense;
- l'organisation d'une réflexion pour le développement d'une filière industrielle africaine axée sur le domaine cybernétique, de manière à diminuer la dépendance vis-à-vis des produits physiques, logiciels et cognitifs développés par les puissances cybernétiques.
- la mise sur pied d'une plateforme de formation, d'éducation et d'exercices de cyber-défense, dont les budgets de fonctionnement, de recherche et d'investissement doivent être exclusivement africains. Cette mesure est de nature à concrétiser les impératifs de formation et de mutualisation des moyens ;
- la promotion de l'adoption du nom de domaine e.Africa, lancé officiellement le 3 juillet 2017, qui se veut l'identité numérique du continent. Cette proposition permettrait de préciser les contours de la souveraineté numérique africaine ;
- l'intensification du développement des infrastructures d'interconnexion et d'hébergement de données sur le continent. Dans ce cadre, il est primordial de favoriser la mise en place des serveurs et des Data-Center sur les territoires des Etats africains, au moins pour les données sensibles des gouvernements, dans le cas idéal pour les données personnelles.
- le renforcement de la coopération avec les partenaires internationaux concernés, particulièrement à travers l'échange des bonnes pratiques en matière de gestion de crise

CONCLUSION

Le champ des études sur la Sécurité s'est élargi avec la consécration du Cyberespace comme un théâtre de confrontation à part entière, au même titre que la Terre, l'Air, la Mer et l'Espace.

Ce faisant, la cyber-conflictualité qui en découle n'est plus perçue comme un affrontement de technologies mais comme un moyen, un autre, en plus, et/ou en complément, des formes de combat cinétiques et létaux, pour réaliser des objectifs stratégiques.

Par ailleurs, l'espace numérique, devenu un espace de tensions culturelles, politiques, sécuritaires et économiques, offre un nouveau cadre pour le jeu des rivalités et de coopération entre acteurs stratégiques, avec pour conséquence une reconfiguration des rapports de forces sur la scène internationale.

Dans ce contexte, les pays africains qui ont réussi, relativement, à amorcer leur digitalisation ont appréhendé, à quelques exceptions, le cyberespace administrativement, sans prendre conscience des conséquences négatives d'un déficit opérationnel sur leur sécurité nationale.

Certes, des mesures préventives et de protection ont été entreprises pour combattre la cybercriminalité qui gangrène le continent, particulièrement dans son espace subsaharien. Cependant, l'ampleur du mal est telle que seule une approche continentale et holistique peut en réduire la propagation.

La même approche doit guider la mise en place d'une cyber-défense africaine, talon d'Achille du cyberespace africain, pour permettre aux pays africains de sauvegarder leur souveraineté numérique et de développer une résilience numérique.

Annexe

Aperçu sur les cyber-attaques annoncées depuis 2007

Années	Evénements survenus
2007	• Une cyber-attaque cible l'Estonie causant un déni de service prolongé de ses infrastructures stratégiques, des banques et des journaux, sur fond de tension avec la Russie
2008	• La Géorgie en conflit avec la Russie subit de vastes cyber-attaques handicapant toutes les infrastructures de ce pays.
2009	• Plusieurs sites gouvernementaux Sud-coréens sont ciblés par des attaques à grande échelle, sur fond de tensions avec la Corée du Nord
2010	• Une cyber-attaque a mis hors d'état de fonctionnement la centrale nucléaire de Bouchehr. Les Etats-Unis et Israël sont soupçonnés d'être derrière cette attaque
2011-2012	• Le constructeur américain «Lockheed Martin» a été victime d'une cyber-attaque massive qui a paralysé ses systèmes informatiques pendant plusieurs heures • Plusieurs comptes Gmail de hauts fonctionnaires américains, des dissidents chinois, des responsables de plusieurs pays asiatiques, des journalistes ont été piratés. Google a déclaré que l'origine de l'attaque est Jinan en Chine. • Une vague d'attaques informatiques cible plusieurs sites gouvernementaux japonais • Une cyber-attaque d'envergure a ciblé des banques américaines, européennes et latino-américaines, causant la perte de plus de 80 millions de dollars • Une cyber-attaque cible les systèmes informatiques de plusieurs firmes énergétiques saoudiennes, attribuée au gouvernement iranien. (Virus Shamoon)
2014	• Un groupe de hackers iraniens a piraté et volé des données confidentielles d'un groupe de loisirs américain dont le propriétaire avait suggéré de raser Téhéran sous le feu nucléaire • Le groupe Sony renonce à la sortie d'un film sur un complot fictif de la CIA pour assassiner le président Nord coréen Kim Jong-Un, suite à un vol massif de ses données informatiques
2015	• La chaîne de télévision «TV5 Monde» est victime d'une cyber-attaque entrainant l'arrêt de la diffusion de ses programmes • Le compte Twitter du Commandement américain au Moyen-Orient (Centcom) a été piraté par des membres de l'''Etat islamique''. • Envoi de menaces de mort, via Facebook, à cinq épouses de militaires américains.
2016	• La Banque centrale du Bangladesh, victime d'un piratage informatique, a perdu 81 millions de dollars. • Une banque équatorienne est attaquée et a perdu 10,7 millions d'euros • La Russie est accusée d'ingérence dans les élections présidentielles américaines
2017	• Une cyber-attaque de grande envergure (Wanacry) paralyse les ordinateurs de multinationales et de services publics d'une centaine de pays (système de santé britannique, ministère russe de l'intérieur, des entreprises) et fait plus de 200 000 victimes. • Une cyber-attaque (Adylkuzz) s'attaque aux ressources des ordinateurs pour y faire du cryptomoning. L'attaque fait des centaines de milliers de victimes • Une cyber-attaque d'envergure (NotPetya) a ciblé, initialement, des entreprises majeures en Ukraine, paralysant une centaine d'entreprises mondiales. • L'essai d'armes cybernétiques russe perturbe le réseau téléphonique de la Lettonie

2018	• L'infrastructure informatique russe et iranienne est la cible d'attaques informatiques avec des répercussions sur les fournisseurs des services internet et les centres de données • La banque HSBC révèle que des comptes bancaires en ligne de ses clients ont été l'objet d'attaques informatiques • Le ministère français des affaires étrangères annonce qu'il a été l'objet d'une opération de piratage de sa messagerie email.
2019	• Des documents appartenant à des responsables politiques allemands sont publiés en ligne • Airbus annonce avoir été victime d'une intrusion dans le système d'information de sa branche avions commerciaux • Les forces de défense israéliennes ont twitté sur leur Compte officiel «nous avons contrecarré une tentative d'attaque cyber de Hamas contre des cibles israéliennes, en frappant l'immeuble utilisé par les hackers de Hamas» • Les Etats-Unis lancent des cyber-attaques contre l'Iran

Type de cyber-nuisance en fonction de la nature de l'acteur concerné.

	Etats	Acteurs non étatiques	Acteurs économiques	Acteurs inconnus
Etats	Cyber-conflit	Cyber-crise Cyber-crime Cyber-terrorisme Cyber-conflit	Cyber-crime Cyber-crise Cyber-espionnage Cyber-conflit	Cyber-crise
Acteurs non étatiques	Cyber-crise Cyber-crime Cyber-terrorisme Cyber-conflit	Cybercriminalité Cybercriminalité aggravée	Cybercriminalité Cybercriminalité aggravée	
Acteurs économiques	Cyber-crime Cyber-crise Cyber-conflit	Cybercriminalité Cybercriminalité aggravée	Cyber-concurrence Cybercriminalité	
Acteurs inconnus	Cyber-crise			

Bibliographie Sélective :

1. Ouvrages

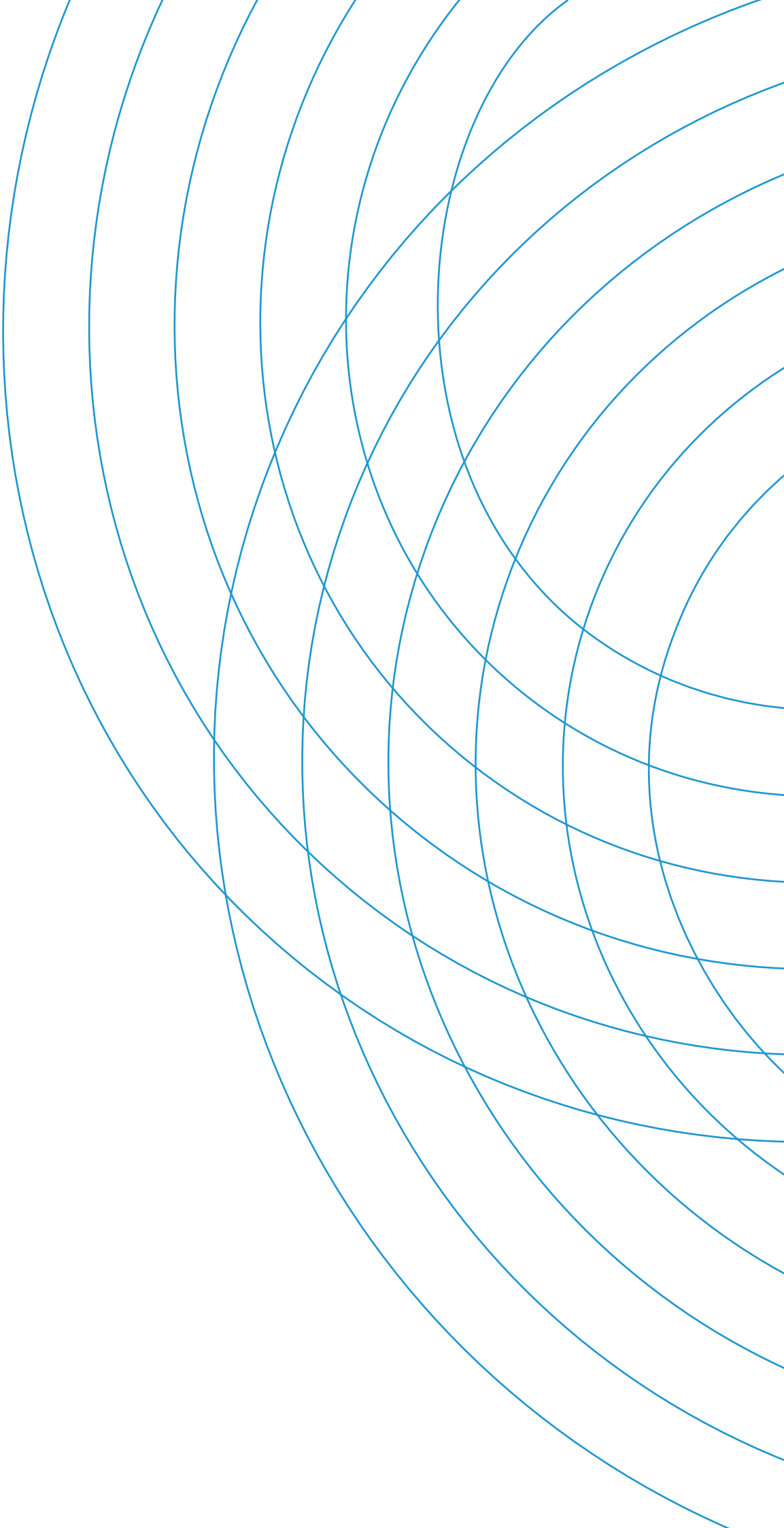
- Francois-Xavier Djimgou «Souveraineté numérique et cyber-défense : un enjeu de taille pour l'Afrique». Editions Edilivre. 2019 .
- Jean Baptiste Eyoukeliye kogoe «les défis de la dématérialisation en Afrique» Editions Edilivre.2019
- Amael Cattaruzza «Géopolitique des données numériques,» Editions le cavalier bleu. 2019
- Marc-Antoine Pérouse de Montclos, «l'Afrique, nouvelle frontière du djihad», éditions la découverte. 2018
- Ministère Français de l'Europe et des Affaires étrangères «les manipulations de l'information» août 2018
- Jean-Louis Gergorin. Léo Issac-Dognin.»Cyber. La guerre permanente.» Les éditions du Cerf. 2018.
- Stéphane Taillat, Amael Cattaruzza, Didier Danet. «la Cyberdéfense, politique de l'espace numérique» Editions Armand Colin. 2018.
- P.W.Singer, Emerson T. Brooking «Likewar. The weaponization of social media». Editions HMH. 2018
- Nicolas Arpagain. «la Cyber-sécurité». ITCIS éditions. 2014.
- Alix Desforges : les représentations du cyberespace : un outil géopolitique. Editions Hérodote 2014.
- Thomas Rid «Cyber war will not take place» Editions Oxford. 2013.
- Daniel Ventre «Cyberespace et acteurs du cyber conflit» Editions Lavoisier. 2011
- Joseph S. Nye «Power and National Security in cyberespace» in America's cyber future, Security and Prosperity in the information Age. Juin 2011.

2. Articles et documents

- Antoine Vandevoorde «Afrique numérique : un état des lieux du cyberespace africain». Site «les yeux du monde.fr», 12 mars 2019.
- Ecofin hebdo, «l'explosion des fake news en Afrique, une menace pour la paix sociale et la pérennité des réseaux sociaux.» Article publié le 14 février 2019.
- Agence Ecofin «Important déficit de datacenters en Afrique subsaharienne».2019
- Rapport d'information de l'Assemblée Nationale française, intitulé «la cyber-défense», enregistré à l'Assembleé le 04 juillet 2018
- Revue Française stratégique de cyber-défense. 12 février 2018.
- National Cyber Security Index 2018.
- Journal «le Monde», intitulé «Chefs d'Etat, diplomates, hommes d'affaires, le Who'Who des écoutes britanniques en Afrique.» .08 décembre 2016.

3. Sites internet

- www.africacert.org
- www.defense.gouv.fr
- Site web du Conseil de l'Europe : www.coe.int.
- www.internetworldstats.com
- Observatoire du monde cybernétique.
- ANSSI, Défense et Sécurité des Systèmes d'information. www.ssi.gouv.fr.



Policy Center for the New South

Complexe Suncity, Immeuble C,
Angle Boulevard Addolb et rue Albortokal,
Hay Riad, Rabat - Maroc.

Email : contact@policycenter.ma
Phone : +212 5 37 54 04 04
Fax : +212 5 37 71 31 54
Website : www.policycenter.ma