2022
004

Ecole Internationale des
Forces de Sécurité
(EIFORCES)

Médiacratie Cybernetique et Menaces Sécuritaires

Enjeux, Défis et Réponses à l'ère de la Digitalisation

Actes du colloque International de Yaoundé organisé par l'EIFORCES les 28 au 29 Avril 2022 au Palais des Congrès

AXE 1 :

La nouvelle donne insécuritaire à l'ère du numérique et des médias sociaux

AXE 2 :

Médias sociaux et numérisation : dilemme «risque-opportunité» sécuritaire

AXE 3 :

Internet et médias sociaux: de l'état de nature au retour à l'ordre

AXE 4 :

Quel avenir sécuritaire, quelle communication et quel développement à l'ère des menaces liées à la médiacratie cybernétique?

RASI
Revue Africaine de Sécurité Internationale

TABLE DES MATIÈRES

RASI est une publication du
Centre de Recherche et de Documentation de l'EIFORCES

Chercheur

M NJIFON Josué,
Chef Service Traduction et Interprétariat à l'EIFORCES

M. ABANDA DANG Marcel Boris,
Assistant de projets à l'EIFORCES

M. NENENGA Driscole AGBORSUM
Assistant de recherche et de traduction à l'EIFORCES

Mlle NDZIE Marie Joseph Norbertine,
Assistante de projets à l'EIFORCES

IP2 NGAMNGOUO Albertine,
Chef du Secrétariat du Centre de Recherche et de Documentation de l'EIFORCES

Mme NGOBO ATEMENGUE Annick épouse TAYOU KAYO,
Diplomate

ONT COLLABORE A CE NUMERO

M. Joseph BETI ASSOMO,
MINDEF PCA EIFORCES

ETOGA Galax Landry
SEDGN

Général de Brigade BITOTE André Patrice

Pr Laurent-Charles BOYOMO ASSALA

Professeur MINKOA SHE Adolphe

Pr Bernard-Raymond GUIMDO

Professeur OLINGA Alain Didier

Professeur Alice NGA MINKALA

Professeur Jean NJOYA

Professeur George BELL BITJOKA

Professeur Alain KENMOGNE

Professeur Désiré AVOM

Professeur Guy MVELLE MINFENDA

Professeur Justine DIFFO TCHUNKAM

Professeur Pierre Etienne KENFACK

Professeur François ANOUKAHA

Dr Commissaire Divisionnaire PASSO SONBANG Elie,

Dr BABA WAME

Dr Wolfgang Fernand Junior OWONA

Commissaire Divisionnaire, Dr Thierry MEDOU

Capitaine de Vaisseau Cyrille Serge ATONFACK NGUEMO

Mme Françoise EKOLLO

Lieutenant-Colonel Brice MIMBOLO

Mme Pierrette EVINA

M. Prosper DJOURSOURBO PAGOU

M. MASSIMA Jean Jacques

EDITORIAL

André Patrice BITOTE
Général de Brigade
Directeur Général de l'EIFORCES

Le Colloque international organisé par le Centre de Recherche et de Documentation de l'EIFORCES, sur le thème : **«MEDIACRATIE CYBERNETIQUE ET MENACES SECURITAIRES : ENJEUX, DEFIS ET REPONSES A L'ERE DE LA DIGITALISATION»** a été financé par l'Etat du Cameroun, dans sa constante sollicitude à l'endroit de l'EIFORCES. En témoigne, la profonde mutation que connaît actuellement le campus d'Awaé, transformé en un vaste chantier.

D'emblée, je tiens à remercier Monsieur le Ministre Délégué à la Présidence chargé de la Défense, Président du Conseil d'Administration de l'EIFORCES, pour avoir autorisé et facilité la tenue de cette importante activité scientifique et professionnelle.

Ma gratitude s'adresse également à vous, Modérateur général, Modérateurs de panels, Rapporteur général, intervenants, discutants, participants et illustres invités, issus de diverses sphères institutionnelles, professionnelles et géographiques, qui répondez favorablement à notre invitation. Recevez, à travers ma personne, les souhaits chaleureux de bienvenue de l'ensemble des personnels de l'EIFORCES.

Je salue particulièrement la présence des auditeurs du 8ème cycle du Brevet d'Etudes Supérieures de Sécurité, originaires du Cameroun, du Congo, de la Côte d'Ivoire, du Mali et du Togo, qui séjournent actuellement à l'EIFORCES. Leur participation à ce colloque est la preuve de l'existence d'une synergie

entre le Centre de Recherche et de Documentation et la Direction des Etudes, dans l'accomplissement des missions statutaires de l'EIFORCES que sont la formation et la recherche dans les domaines de la sécurité et du maintien de la paix. La recherche - c'est un truisme - constitue un précieux adjuvant à la formation.

Le présent Colloque est en parfaite adéquation avec la mission de recherche et de veille stratégique et prospective de l'EIFORCES dans le champ de la sécurité globale. Il convient, à ce sujet, de rappeler, qu'une réflexion analogue avait été menée, du 5 au 8 décembre 2018 à Douala, dans le cadre d'un séminaire organisé par l'EIFORCES avec le soutien du Japon, via le Programme des Nations Unies pour le Développement, sur le thème : « **DEFIS ET ENJEUX DE LA CYBERCRIMINALITE ET DE LA CYBERSECURITE EN AFRIQUE CENTRALE** ».

Cest dire que la problématique prégnante, connexe et autant complexe de la «**médiacratie cybernétique**» et des menaces y relatives, se situe dans la continuité du séminaire de Douala, et trouve son fondement dans les transformations et reconfigurations opérées au sein de l'espace virtuel, avec la mondialisation sans cesse croissante des échanges et le développement fulgurant de la communication digitale.

Aussi, les présents travaux, que je souhaite intenses et fructueux, représentent-ils une opportunité de mutualiser des intelligences et compétences diverses dans l'optique, d'une part, de minimiser, à défaut de neutraliser le potentiel déstabilisant de ces médias, et, d'autre part, de repenser et d'optimiser leur utilisation, dans une perspective vertueuse, citoyenne et responsable.

Je prie Monsieur le Ministre Délégué à la Présidence chargé de la Défense, Président du Conseil d'Administration de l'EIFORCES, de bien vouloir transmettre à Son Excellence Monsieur le Président de la République du Cameroun, Chef des Forces Armées et Chef Suprême des Forces de Police, notre déférente reconnaissance pour les hautes et incessantes attentions qu'il porte à l'EIFORCES, qui mettra toujours un point d'honneur à les capitaliser.

ALLOCUTION D'OUVERTURE

Monsieur Joseph BETI ASSOMO
Ministre Délégué à la Présidence chargé de la Défense
Président du Conseil d'Administration de l'EIFORCES

C'est avec un plaisir renouvelé que je vous souhaite la bienvenue dans cette somptueuse salle du Palais des Congrès de Yaoundé, cadre du Colloque International, organisé par l'Ecole Internationale des Forces de Sécurité (EIFORCES) sur le thème «**MEDIACRATIE CYBERNETIQUE ET MENACES SECURITAIRES : ENJEUX, DEFIS ET REPONSES A L'ERE DE LA DIGITALISATION**».

Initiative portée par le Centre de Recherche et de Documentation de l'EIFORCES, j'ai accueilli ce projet avec un grand intérêt, tant son objet s'inscrit dans l'actualité et tient compte des défis sécuritaires auxquels doivent faire face la plupart, sinon l'ensemble des pays africains. En effet, l'homme moderne se distingue par son appétence à la consommation médiatique. La place des médias dans les sociétés contemporaines ne fait l'objet d'aucun doute. Qu'on les abhorre ou au contraire qu'on les adule, la réalité est qu'ils sont là, nous contraignant à composer avec eux, du fait des multiples rôles qu'ils remplissent : information, éducation, divertissement, pour ne citer que ceux-là.

Si l'appropriation rapide de la digitalisation est une réalité, des dérives sont observées dans l'utilisation faite de ces technologies de l'information et de la communication : fake news, discours haineux, violence verbale, attaques cybernétiques, etc.

Au Cameroun comme dans le reste des pays du monde, le pouvoir des médias se renforce au fil du temps, à la faveur des avancées technologiques. A la presse écrite, s'est ajoutée la radio, ensuite la télévision et, aujourd'hui, les médias

cybernétiques (réseaux sociaux, blogs…), qui sont les marqueurs de notre temps.

Avec ces médias cybernétiques, on assiste à un partage rapide et continu de l'information qui échappe très souvent aux normes éthiques et aux critères de validité d'une information de qualité, à savoir l'exactitude, la justesse et la sincérité.

L'on comprend alors l'appel du Président de la République, S.E Paul BIYA, lancé à la jeunesse, lors de son Discours du 11 février 2022, à un «usage responsable, instructif et constructif des réseaux sociaux, dont la vocation première est d'offrir des espaces et des opportunités d'échange, d'information et de communication dans des domaines les plus variés».

Le temps d'une allocution ne suffirait pas à égrainer toutes les dynamiques de la médiacratie cybernétique et leurs inférences dans le champ sécuritaire.

Les menaces y relatives sont de nature à porter atteinte à la sûreté de l'Etat, à la sécurité des personnes et des biens, et à fragiliser le tissu économique en mettant en difficulté de nombreuses entreprises.

Le Colloque International qu'organise le Centre de Recherche et de Documentation, dans le cadre du plan de performance administrative 2022 de l'EIFORCES, est donc au cœur des enjeux et défis sécuritaires de l'heure.

Je n'ai nul doute que cette importante activité scientifique, qui interpelle aussi bien les acteurs du secteur public que du secteur privé, apportera une meilleure compréhension et des solutions efficaces à ces nouvelles formes de menaces.

Il est aujourd'hui plus qu'important que les termes issus du vocabulaire numérique et du développement des médias dans l'espace virtuel comme « médiacratie», «fake news», «cryptomonnaie» soient compris par tous, afin de savoir à quelles formes de menaces on doit faire face, et partant de mieux s'en prémunir ou d'y apporter des solutions efficaces.

Que ces deux jours soient riches en enseignements et nous édifient davantage sur les dynamiques médiacratiques et leurs inférences dans le champ sécuritaire. Sur ce, en émettant le vœu qu'ils débouchent sur des recommandations concrètes, je déclare solennellement ouverts les travaux de ce Colloque International.

Vive le Cameroun et Son Illustre Chef, Son Excellence Monsieur Paul BIYA, Chef des Armées et Chef Suprême des Forces de Police.

Je vous remercie. / -

PRÉSENTATION DE L'ACTIVITÉ, DE SA PROBLÉMATIQUE ET DES PANELS

Docteur Elie PASSO SONBANG
Commissaire Divisionnaire
Chef du Centre de Recherche et de Documentation de l'EIFORCES

Je suis honoré ce matin de prendre la parole devant cet auditoire pour présenter l'activité scientifique qui nous réunira pendant deux jours dans cette majestueuse salle du Palais des Congrès de Yaoundé.

Le Centre de Recherche et de Documentation (CRD) de l'EIFORCES, Direction Stratégique et Opérationnelle de l'Institution en matière de recherche, pilote plusieurs activités scientifiques d'envergure, ancrées dans les défis sécuritaires contemporains. Les publications à caractère scientifique et l'organisation des colloques sont les plus régulières et inscrivent le CRD de l'EIFORCES dans l'agenda des rendez-vous importants du savoir aux niveaux national et international. En effet, depuis quelques années, le CRD n'organise pas moins d'un colloque par an, toujours en lien avec les challenges sécuritaires du moment pour, coller à la notoriété de l'Ecole, celle d'une expertise africaine et internationale de référence en matière de sécurité et de paix au service de l'Afrique et du monde.

Fidèle à cette tradition, qui fait dorénavant sa réputation et l'impose parmi les cercles crédibles de réflexion en matière de sécurité nationale et internationale, l'EIFORCES se penche cette année, à l'occasion de sa rentrée scientifique, sur un fait majeur de notre société, la médiacratie cybernétique.

Le Colloque International qui s'ouvre ce jour est organisé sur le thème : **«MEDIACRATIE CYBERNETIQUE ET MENACES SECURITAIRES: ENJEUX, DEFIS ET REPONSES A L'ERE DE LA DIGITALISATION»**, intervient donc à un moment crucial où, au Cameroun comme dans la plupart des pays du monde, les dérives observées sur les

réseaux sociaux et autres médias en ligne connaissent un développement exponentiel aux conséquences parfois dramatiques pour les personnes physiques et morales.

Inscrite dans la planification des activités de recherche de l'EIFORCES, pour le compte de l'année 2022, cette problématique interpelle, d'autant plus qu'elle questionne nos rapports avec ces outils technologiques et de communication. Au surplus, elle interpelle sur le rôle des médias, en général, et des médias cybernétiques, en particulier, dans nos sociétés ; notamment dans leurs interactions avec les autres composantes de la société. Les médias font donc corps avec nous et ils gagnent davantage en influence du fait même que dans la dynamique civilisationnelle, ils sont désormais les baromètres de notre société. De fait, les médias constituent « un quatrième pouvoir », si l'on veut compléter la conception de Montesquieu de la séparation des pouvoirs dans l'Etat.

A travers ce Colloque International, l'EIFORCES entend questionner la corrélation qui pourrait être établie entre la propagation des nouvelles formes de menaces et l'avènement de l'ère digitale. Il est donc question de se demander en quoi la libéralisation poussée du cyberespace hypothèque-t-elle la sécurité, gage du développement de tout Etat ?

Telle est ainsi énoncée la problématique qui sous-tendra cette activité organisée par l'EIFORCES, instrument de la politique publique au service de l'Etat et de la Communauté Internationale dans les domaines de la sécurité et du maintien de la paix.

Durant ces travaux, qui tiendront sur deux jours, un groupe d'experts du cyberespace et des medias cybernétiques issus du champ universitaire, du champ professionnel de la sécurité, des systèmes d'information et de la communication, va s'y pencher en mettant en lumière, les constats, les enjeux et les perspectives théoriques et pratiques, ceci autour de quatre axes thématiques repartis en 4 modules :

- **Module 1** : **«La nouvelle donne insécuritaire à l'ère du numérique et des média sociaux» ;**
- **Module 2 : «Médias sociaux et numérisation : dilemme « risque-opportunité » sécuritaire» ;**
- **Module 3 : «Internet et médias sociaux : de l'état de nature au retour à l'ordre» ;**

- **Module 4 : «Quel avenir sécuritaire, quelle communication et quel développement à l'ère des menaces liées à la médiacratie cybernétique ?».**

Il s'agira, pour ces experts:

- d'apporter des précisions terminologiques sur le concept de médiacratie cybernétique ;
- de mettre en exergue les fondements théoriques, juridiques, épistémologiques et stratégiques de la problématique à examiner ;
- de répertorier les médias sociaux, digitaux, les plus perméables aux usages faits par des entrepreneurs directs ou indirects d'insécurité ;
- d'identifier les entrepreneurs d'insécurité les plus cyber représentés, ainsi que les modes opératoires privilégiés par les groupes jugés à risque dans leur déploiement au niveau des médias cybernétiques ;
- d'évaluer l'impact des usages potentiellement dangereux sur l'évolution perceptuelle et réelle des crises et des risques sécuritaires;
- de dresser le bilan critique des mécanismes de régulation existants en matière d'encadrement des usages des TIC ;
- de suggérer des voies d'amélioration des pratiques et des mécanismes de contrôle et de régulation des comportements des acteurs au sein du cyberespace.

Le colloque qui s'ouvre aujourd'hui, ambitionne d'apporter une meilleure compréhension de ce phénomène, sans conteste, menace majeure de notre temps. Nous sommes convaincus qu'il en sortira, au regard de la qualité des intervenants, les clés et les recettes qui aideront à mieux saisir et encadrer le phénomène cyber-médiatique. Les réponses aux préoccupations lancinantes, aux inquiétudes affolantes de l'agressivité des cybermedias seront certainement mises en exergue. Nous dessinons, dès ce jour, pour l'avenir, les contours d'une société capable, tout en capitalisant leurs bienfaits, d'annihiler le potentiel de nuisance sécuritaire des medias cybernétiques.

En nous souhaitant de fructueux travaux, je vous remercie de votre attention. /-

LEÇON INAUGURALE: LE VIVRE ENSEMBLE DANS UN MONDE CONNECTE: REMARQUES A PARTIR DE L'AFRIQUE

Professeur Laurent-Charles BOYOMO ASSALA
Professeur Emérite des Universités

La science dominante, gonflée de modernisme et de technocratie semble avoir consacré l'idée d'une sorte de «*suma divisio*» entre la pensée primitive, intuitive et sensorielle, caractéristique des sociétés traditionnelles, et l'appréhension moderne, ingénieuse et créatrice du monde contemporain. Malgré les efforts de l'anthropologie et de l'ethnologie en vue de réhabiliter les sociétés anciennes, en montrant l'extrême complexité de la production totémique comme preuve de l'inexistence d'une pensée primitive par exemple, la conviction reste forte que la science moderne, dynamique et réfutable, offre une connaissance plus adaptée aux besoins contemporains que ne peut l'être la pensée sauvage, statique et empirique. L'avènement du cyberespace a plus encore que par le passé exacerbé l'idée que, malgré sa prétention à l'universalité, l'esprit des mutations complexes appartient à certaines sociétés plus qu'à d'autres, les idéologies partisanes étant venues creuser plus encore dans le sillon de la division internationale de la connaissance scientifique et technique. Bien que l'espace cybernétique ait été présenté spontanément comme un «*no man's land*», sorte d'espace interchangeable où l'être humain reste anonyme selon Marc Augé, l'internet et sa domiciliation en des lieux de production restent clairement circonscrits au Nord de notre planète. S'il peut paraître nécessaire de s'attaquer à ces erreurs historiques et anthropologiques et à la littérature requalifiant qui les

promeut, l'universalité du grand partage dont la prospérité reste tout aussi portée par une utopie universaliste ne peut pas constituer un argument décisif pour ceux qui scrutent la place marginale de l'Afrique dans le concert des nations modernes.

Comment le nouvel espace virtuel prend-il sens en Afrique aujourd'hui, qui plus est, dans un contexte d'exacerbation et de radicalisation de la violence meurtrière et de haines vertigineuses entre les peuples? Quels seront les contours de la citoyenneté nouvelle que nous voyons éclore chaque jour et avec les moyens de la virtualité? Cette cyberréalité qui s'élabore sous nos yeux peut-elle être porteuse de sens nouveau pour l'Afrique? Bien que les lignes de réflexion dessinées par la présente leçon s'inscrivent dans un débat très large, au croisement de nombreuses questions sociologiques et épistémologiques et qui ont assuré la compétition thématique de nombreuses rencontres scientifiques, nous nous bornerons à n'évoquer que quelques grandes questions qu'il s'agit de mettre en débats au cours du présent colloque. A rebours des thèses de la liberté et de l'égalité comme principes fondamentaux de qualification de la démocratie pluraliste, nous posons la catégorie du retournement numérique qui s'émancipe aux frontières des hymnes à la liberté et accessoirement à l'égalité pour inciter à penser un contre-discours sociocritique de l'intelligence démocratique. Nous posons comme hypothèse qu'une sorte de radicalisme inspire l'imaginaire cybernétique qui, tout en invoquant le principe de liberté et l'idéal d'émancipation des peuples, s'attaque aux fondements même de ceux-ci. Le retournement numérique est, dans ce contexte, une sorte de praxis cognitive propre à décomplexer le regard africain sur le cybermonde et à en tirer le plus grand avantage.

En nous appuyant sur le cadre d'un processus interactionniste et postmoderniste engendrant un retournement numérique, nous entreprenons de redéfinir le vivre ensemble comme une utopie créatrice (1) qui se propose de dépasser les catégories classiques qui surgissent de la réflexion sur la fracture entre nantis et démunis du numérique (2) notamment quand on y fait référence à l'Afrique.

1 - LE CYBERMONDE ET SES UTOPIES

De fait, les concepts qui fondent ma présentation et qui m'ont été aimablement proposés par les organisateurs ne peuvent raisonner que dans les catégories de l'idéalité. A la limite, ils pourraient même relever de l'utopie qui, comme on le sait, est de l'ordre de «l'imaginaire prédictionnel et non prévisionnel». Comme l'observe Julien Freund, l'utopie, qui est une pensée insulaire et qui «méconnaît tout rapport au voisinage, et ne tient pas compte de l'ennemi extérieur», l'utopie disais-je, présuppose le bien par éradication du mal, l'abondance économique en éliminant les problèmes de rareté, donc les besoins de production, de concurrence ou d'exploitation (Freund, *L'espace dans les Utopies*, Grenoble, PUG, 1979). La formulation banale de ladite idéalité renverrait à un choix entre le bien (civilité conviviale) et le mal (état de nature) en s'obligeant à condamner ou à louer à priori et indépendamment des positions sociales des acteurs et des conditions historiques dans lesquelles lesdites positions s'insèrent. C'est donc, l'exploration du champ dans lequel s'inscrit ce cybermonde rêvé qui nous préoccupe ici et qu'il faut rapidement délimiter en désignant ses concepts fondamentaux, et examiner ses conditions de possibilité dans le cadre d'une redéfinition de sa structure instrumentale et normative et de ses irradiations dans la vie quotidienne. Rappelons, à cet égard, que l'interactionnisme symbolique s'oppose aux vérités absolues. **Il soutient qu'il n'y a pas une vérité unique, mais des vérités différentes**. Pour comprendre ces différentes «vérités» dont aucune ne s'accuse par l'évidence, l'interactionnisme étudie les relations entre les personnes et les symboles, le but ultime étant de comprendre l'identité individuelle dans ses rapports avec l'organisation sociale.

1.1 - LES TROIS PIÈGES DE L'ÉPISTÈME CYBERNÉTIQUE

Je souhaite d'une part, évoquer les trois pièges principaux que tend l'intitulé de cette rencontre, trois termes et groupes de mots –civilité conviviale, viatique et état de nature-qui ne sont pas nécessairement complémentaires ni dépourvus de contradiction entre eux. Et qui plus est, ils peuvent apparaître comme porteurs précisément de ces évidences dont il

convient de se départir: en premier lieu, celui de la réduction de l'espace cybernétique à sa dimension indicielle et instrumentale, destinée à recevoir tous les contenus y compris les plus absurdes et en particulier ceux dont l'abjection est favorisée par les avantages de l'anonymat de leurs auteurs. Dans ces conditions où le cybermonde n'est alors que l'instrument et le support de sens que suggère les usages décomplexés ou indociles d'internet, l'hypothèse de la civilité s'éloigne pour laisser place à une reproduction d'un l'état de nature d'autant plus violent qu'il n'offre plus la possibilité même aux plus forts, d'imposer leurs lois, et ne laissent survivre et triompher que ceux que la nature a doté de capacités psychologiques susceptibles de supporter tous les déjections qu'il est possible de produire. Ou, à contrario faut-il se garder du réflexe de penser l'alternative de la civilité et de l'état de nature en termes de conséquences résultant du bon ou du mauvais usage de la cybernétique en déniant le caractère historique et socioculturel de son appropriation. Ce serait le deuxième piège d'appréciation historique de cet intitulé. Associé au premier, ces pièges répudient aisément l'irréfutabilité de la domiciliation occidentale et en tout cas fortement septentrionale de la technologie du numérique. Quant au troisième piège, celui d'un retour à l'état de nature historiquement impossible mais envisagée comme une hypothèse stimulante pour penser les limites d'un sentiment de liberté, sentiment qui serait la nourriture ultime – le viatique donc- du voyage vers et dans l'espace cybernétique. Si liberté il y a dans le cybermonde, disons-le tout net, celle-ci est plus ressentie dans l'expérience de pensée et dont la structure langagière semble relever du sacré.

Une fois ces erreurs épistémologiques circonvenues, il faut, d'autre part, faire face à un autre défi, non moins important, celui du totalitarisme cybernétique. *«Le totalitarisme peut se définir,* précise Vioulac*, comme pouvoir de la Totalité sur toute particularité, et bien plus comme dissolution de la particularité dans la Totalité, par laquelle la Totalité conquiert la puissance totale nécessaire à l'exercice de son pouvoir. L'avènement d'une puissance absolue, illimitée, qui ne rencontre jamais que les limites qu'elle se fixe elle-même»* (Jean Vioulac, *La massification***.** *Tocqueville et le totalitarisme démocratique***,** La logique totalitaire, (2013). La figure du cybernétique se dessinerait dans cette perspective au mieux comme une alternative entre le bien et le mal, et au pire comme une injonction improbable de la promesse d'une totalité instituante.

1.2 - UN CYBERMONDE ENCHANTÉ

La protubérance conceptuelle du cybermonde reflète, aujourd'hui, des conceptions différenciées des technologies numériques dans la relation à la société et l'enchantement de l'internet qui s'est produit dans les années 2000. Deux répertoires d'action numériques forment le corpus d'affectation positive de ce monde, à savoir la nouvelle économie créative qui en découle et le type de citoyenneté dans lesquels il convient de situer les théories que nous allons présenter ici. Ces deux catégories de la pensée numérique sont, cependant, affectées de manière différente. Premièrement, ceux qui sont pour ce nouvel univers insistent sur ses atouts multiples en évoquant le basculement du monde vers une économie de la création qui démonopolise le capital. Si le rapprochement de la cybernétique avec le totalitarisme n'est pas nouveau, Maxime Ouelet est de ceux qui en donnent plutôt une image économique enchantée. Depuis une quarantaine d'années, écrit-il, l'application des principes de la cybernétique au fonctionnement des marchés a considérablement accru le potentiel totalitaire du capital. Rappelant que la cybernétique se définit comme la science de la régulation sociale et de l'optimisation des ressources informationnelles – en somme, la science du contrôle par la communication, Ouelet évoque Friedrich Hayek, le principal idéologue de la doctrine néolibérale, lequel est à l'origine du «manifeste» de la révolution cybernétique en économie. «Selon lui, le marché ne se caractérise pas par sa capacité d'établir un équilibre parfait entre l'offre et la demande; il s'agit plutôt d'une gigantesque machinerie informationnelle qui transmet de l'information aux divers agents économiques, eux-mêmes conçus comme des «processeurs informationnels» censés analyser rationnellement les signaux du marché de manière à maximiser leurs profits. Dans les sociétés capitalistes avancées, dont l'institution centrale est la grande entreprise, l'objectif est plutôt de déterminer d'avance les volontés particulières par des mécanismes de planification de la consommation».

C'est dans ce contexte qu'il faut comprendre le phénomène de *big data* qui se caractérise non seulement par la production de quantités massives de données numériques, mais, surtout, par la capacité des nouveaux outils informatiques d'analyser ces données à des fins prédictives. Les *big data* reposent sur la prémisse qu'il est possible de récolter la totalité des données provenant de la numérisation de l'activité sociale, ce qui rendrait obsolète

l'interprétation des faits sociaux à partir des théories scientifiques puisque le réel parlerait de lui-même. Si le totalitarisme est le monopole de la violence physique et symbolique par un pouvoir ayant perdu son autorité, ce que la cybernétique fait au totalitarisme est que celui-ci tend à s'atomiser, et son niveau de concentration se diluer par désintégration de son centre de gravité. La philosophe allemande de la violence Hannah Arendt disait «Le règne de la pure violence s'instaure quand le pouvoir commence à se perdre». En l'espèce le totalitarisme cybernétique est le transfert de la décision politique, c'est-à-dire de l'autorité, à une oligarchie économique dont la puissance fusionne dans le lexique universaliste de son énonciation.

Deuxièmement, d'autres auteurs, non moins nombreux, évoquent la notion de cyber citoyenneté, *digital citizenship*, pour décrire une *«relation à l'ordre politique au sens large, relation médiatisée par les technologies numériques, et dont les formes, les lieux et les enjeux varient dans le temps et dans l'espace*» (Greffet, Wojcik, 2014: 152). Elle suppose une redéfinition des droits et devoirs des citoyens autour des appropriations des technologies numériques. Dès lors, la citoyenneté numérique, qui pouvait apparaître comme une notion normative positive, visant une société plus égalitaire et démocratique avec le numérique, est désormais conçue sur un mode défensif comme une protection opposable par les publics aux contraintes et rapports de force du déploiement des technologies numériques tel qu'il s'organise depuis la fin du XX^{e} siècle. Pour certains auteurs tels que Greffet et Wojcik, cette conception ferait émerger une troisième définition de la citoyenneté numérique, axée sur la préservation de la vie privée des citoyens, dans un contexte de production et d'exploitation de données massives (*Big data*) à partir des traces numériques des internautes. Il demeure que la citoyenneté du cybermonde tend à reproduire les inégalités du monde réel, aussi bien entre les membres du même Etat qu'entre les Etats eux-mêmes.

2 - LE DIGITAL ET SES FRACTURES

Si le contexte d'usage du numérique a placé le terme fracture– ou fossé – en le marquant du sceau de l'opposition entre ceux qui ont accès au numérique en termes de disponibilité et de qualité et qui en connaissant les usages, et ceux qui en sont écartés pour des raisons sociologiques ou économiques, il a eu peu d'effet sur la glorification qui entoure l'univers de représentations réelles et symboliques du cybermonde. Bien que

fortement affectés par les inégalités numériques, les enjeux socio-économiques, culturels et politiques de ce monde restent encore fortement enchantés par les références normatives de celui-ci, lesquelles sont d'abord indentifiables à travers l'univers sémantique de similarité qui les caractérise (2.1). Sous le masque de la rhétorique, des fractures se dévoile une sorte de métastases qui n'est pas que sémantique mais touche au fondement même de ce nouveau mode de vie (2.2).

2.1 - FRACTURES NUMÉRIQUES, MÉTASTASES LEXICALES

Ce qu'il y a de commun en effet entre le big data et la protection des données personnelles, la transparence vis-à-vis des publics, l'infobésité, le brouillage des frontières entre vie privée et vie professionnelle, la fracture numérique (générationnelle, géographique), la traçabilité, les algorithmes prédictifs et le libre arbitre, n'est-il pas déjà la seule référence en un monde caractérisé par la proximité de ses usages conceptuels ? Cette accumulation d'inutiles synecdoques référentielles et sémiques apporte-t-elle une compréhension additionnelle du cybermonde pour en exprimer les variétés cognitives ? Ou bien la coquetterie des usages similaires a-t-elle pour but ultime de tenir le sens commun en otage ? On pourrait tenter d'expliquer ces cumulations thématiques et les similarités qui couvrent leur imaginaire commun. D'après les définitions canoniques en effet, l'analyse des similarités permet aux données de qualifier elles-mêmes leurs propres structures au lieu que le chercheur détermine à son niveau et *à priori* les catégories sur la base desquelles il travaille. Mais les catégories qui servent de toile de fond à l'analyse des équivalences sont extrêmement complexes quand elles se proposent de déterminer le niveau de proximité et de compétition qui est susceptible d'autoriser leurs comparaisons. Cernées par une profonde ambivalence qui tient de la nécessité de la contextualiser, les catégories deviennent d'inutiles pléonasmes emphatiques et des hyperboles qui mettent en tension l'insistance expressive et la visée argumentative. Comment ne pas évoquer la notion de similarité dans l'analyse du cybermonde tant les catégories qui y font référence sont plurielles et néologiques, et leurs usages similaires et équivalents ? Comment les saisir à partir d'un cadrage fédérateur quand l'univers sociologique et son échelle d'abstraction sont si dynamiques qu'aucune référence théorique ne semble

à même d'en apaiser le dilemme cognitif ?

La cybernétique a ainsi créé des êtres discursifs dont l'équivalence ontologique s'investit dans le système normatif qui les caractérisent et les codes qui supportent ledit système: digital, internet, web, virtuel, etc. Le nouveau lexique suggère l'existence d'un monde parallèle dont les seuls radicaux, web et cyber servent désormais de référence fédératrice, un cybermonde, sa cyberréalité ses logiques et ses codes. Pourtant, la réalité de la cyberréalité africaine suit la distinction que Kling (1998) avait déjà opérée entre le *technical access* et le *social access* pour recouper largement la définition que donnent Brotcorne et Valenduc (2008) suivant laquelle la fracture numérique est la rupture entre ceux qui possèdent et utilisent les outils TIC (téléphone «fixe», portable, ordinateur, Internet) et ceux qui ne les possèdent pas ou ne savent pas les utiliser. Si en Afrique, à peine 10% de la population utilisent internet, le Cameroun se situe, quant à lui, à 5% environ, taux qui cache de profondes disparités en ce qui concerne les usages des mails, recherches en ligne et téléchargement, les communications interpersonnelles (yahoo, facebook), la navigation et le *e-learning*, bien que les effets d'amplification et de propagation soient importants. La leçon à en tirer, ici, est principalement que la défétichisation du cybermonde est d'abord une opération d'hygiène discursive, car pour remplir sa fonction thérapeutique, le langage doit avant toute chose, se soustraire à la structure rationnelle du sacré afin d'atteindre le sens rationnel de la validité normative de l'éthique discursive, comme l'enseigne si bien Habermas.

2.2 - CITOYENNETÉ DIGITALE ET RÉSISTANCES LOCALES

La littérature sur la notion de citoyenneté numérique s'est enrichie ces dernières années des apports théoriques du développementalisme qui était fortement entré en déclin depuis plusieurs décennies. Pour les auteurs de cette thèse, la citoyenneté numérique traduirait «la capacité à participer à la société en ligne» (Mossberger, Tolbert et McNeal, 2008. Suivant la définition qu'en donne notamment de T. Marshall (1950: 11), si la citoyenneté est le fait «de vivre une vie conforme aux standards prévalant dans la société», elle est, alors, susceptible de s'étendre et de se conforter lorsque ces standards évoluent. Dans le contexte contemporain la citoyenneté numérique se conçoit alors comme une extension de la

citoyenneté «ordinaire». Ainsi en dépit des origines libérales de l'internet (Loveluck, 2015), les auteurs de ce courant estiment que les enjeux des inégalités d'accès à celui-ci et de littératie numérique doivent faire l'objet d'interventions étatiques au nom de la dimension morale de l'économie dont Aristote déplorait déjà en son temps la relégation sous le boisseau au profit de sa dimension mécanique. La citoyenneté digitale apparaît donc bicéphale. Elle porte, à la fois, sur l'idée d'une morale économique prônant l'égalité de tous face au numérique, et celle d'un libéralisme démocratique à visage humain sous le contrôle d'un pouvoir public régulateur. Quelles relations avec la violence ? Diriez-vous.

Qu'on se comprenne bien: la violence, qu'elle soit physique à travers le terrorisme, ou symbolique par le biais de la propagande, n'est pas un fait nouveau, et n'est pas plus le marqueur de notre époque tourmentée que d'une autre. Ce qui se joue actuellement c'est son inscription spontanée dans l'univers cybernétique comme la forme dégradée et pervertie de la liberté que ledit univers induit. L'environnement cybernétique et ses célébrations spontanées en sont-ils responsables ? De quelle manière contribuent-ils au dévoilement ou à la fermeture de la violence au regard analytique ? Peuvent-ils favoriser une distribution inégale des formes de violences susceptible de nourrir soit l'hypothèse d'un retour à l'état de nature lequel état aurait fait de la violence sa caractéristique fondamentale, soit celle d'une citoyenneté imparfaite parce que travaillée par les imperfections des politiques publiques du numérique ?

D'abord ceci: **la mise au pas totalitaire appelle de ses vœux son lot d'affrontements violents, notamment physiques, entre le peuple et le pouvoir**. Si les inégalités numériques se résument comme les conséquences d'un accès irresponsable aux infrastructures du numérique et des modes d'usages, d'une part, et de l'inadaptation des systèmes institutionnels de régulation, d'autre part, comment sortir de ce dilemme que l'on a voulu considérer dans cette présentation comme un piège ? La réponse est que l'internet comme face ludique du numérique, offre à ses usagers un sentiment de liberté d'une telle intensité qu'il leur est difficile de l'envisager du point de vue de ses formes hideuses. Comme un serpent qui hypnotise sa proie avant de l'avaler, internet rend la violence numérique euphémique, attirante et souhaitable. Le sentiment de liberté qu'offre l'accès à internet invisibilise la clôture de cet accès à ceux qui manquent de compétences matérielles, intellectuelles et psychologiques pour en comprendre les codes. Or ladite

clôture prend des formes variées selon les circonstances et les milieux. Elle peut ainsi être politique dans des régimes autoritaires, économique devant les situations de précarité, intellectuelle, pour ceux qui ne disposent pas de compétences scientifiques, culturelles et même sociale pour un grand nombre d'individus qui cumulent tout ou partie de ces handicaps.

Or l'idée d'appropriation du numérique vient renforcer le sentiment d'appartenance à la communauté politique (approche républicaine), la participation à la décision publique (approche démocratique) et la lutte contre les inégalités et discriminations, y compris sur le plan économique (approche inclusive de la citoyenneté), précise Mossberger, donnant ainsi le sentiment d'une forme d'équivalence entre le bon internet et le mauvais usage de celui-ci. Pourtant il y a lieu de distinguer et de ne pas confondre le cyberespace utilisé comme outil conceptuel qui rend la figure des mots centrale à l'explication et à la compréhension de notre texte, et l'internet vécu dont l'importance est subordonnée à la validité de ses usages.

Du point de vue qui est le nôtre, et de manière synthétique, il ne s'agit pas de choisir ou de rejeter le numérique et sa forme la plus visible qu'est internet, mais d'en faire un objet public désirable. Car ici, la certitude qu'on a désormais d'être dans un monde nouveau s'impose non seulement comme une nécessité mais aussi comme une valeur et du fait qu'elle est partagée par le monde entier, cette valeur devient moralement bonne. L'objectif est non pas de lui tourner le dos à ce nouveau monde, mais de le retourner sur lui-même afin qu'elle devienne un laboratoire pour penser de nouvelles relations sociales. Un grand nombre de réflexions s'effectuent, en effet, aujourd'hui autour de ce qu'on appelle le retour aux communs, c'est-à-dire le développement des espaces de vie (des tiers-lieux) organisés autour d'un intérêt commun réarticulant la communauté à la société. Ces communs sont plus que des attouchements au cybermonde, car ils reposent sur ce que Weber appelle l'appartenance subjectivement ressentie des acteurs sociaux, et leur attitude. C'est à une critique postmoderne et post coloniale qu'invite, en effet, le paradigme du retournement numérique. Dans la formulation axiomatique du subalternisme, le retournement du numérique nous apparaît donc comme une invitation à la table des puissants de l'internet aux gens d'en bas – les opprimés, les dominés, les subordonnés, les hors caste –, en un mot des subalternes du cybermonde. A défaut de créer un cyberespace exclusif à l'Afrique, les usages domestiques doivent permettre de mettre en place une rhétorique du rapport social qui rend plus proche de nous ce nouvel instrument désacralisé.

PANEL 1: LA NOUVELLE DONNE INSÉCURITAIRE À L'ÈRE DU NUMÉRIQUE ET DES MÉDIAS SOCIAUX

MEDIACRATIE CYBERNETIQUE: GENEALOGIE D'UN CONCEPT ET INFERENCES A L'ERE DE LA MONDIALISATION

Alice NGA MINKALA
Professeur Directeur de l'ESSTIC

INTRODUCTION

Depuis l'avènement des médias sociaux et des réseaux sociaux, l'on peut observer de nombreux bouleversements, caractérisés notamment par l'invasion de l'espace public par une multitude d'acteurs, tous désireux de participer aux agapes de l'information. En effet, les progrès technologiques ont favorisé la création de nouveaux moyens et outils de communication et engendré des médias et des plateformes de partage. Ces innovations simples, souvent mobiles, accessibles en termes de coût, de maniabilité et d'encombrement, et privilégiant le mode participatif, ont également accéléré la circulation de l'information et favorisé le développement de nouvelles pratiques de partage, de diffusion et de mise en relation des individus. Les médias sociaux[1] offrent, aujourd'hui, à tous la possibilité d'accéder à un espace public, pour des échanges, des rencontres virtuelles, et pour le partage et la diffusion rapide de l'information au-delà des lieux

[1] Médias sociaux: plateformes digitales englobant des applications et des fonctionnalités, accessibles par Internet permettant aux utilisateurs de créer, d'organiser et de partager des informations (textes, photos, vidéos, liens...), à l'instar de Facebook, Twitter, LinkedIn, Snapchat, Instagram, Pinterest, YouTube et autres. Les réseaux sociaux sont des sites dont la vocation première est la mise en relation des utilisateurs entre eux (les blogs, les forums ou les wikis), ils constituent donc une infime partie des médias **sociaux**.

physiques de l'événement.

Les nouveaux acteurs de l'espace public ont pris d'assaut les médias sociaux en s'appropriant le cyberespace pour promouvoir une certaine culture démocratique, basée très souvent sur la contestation. Dans cette lancée, les médias sociaux deviennent des moteurs d'émergence d' une nouvelle catégorie d'individus «capables» de jouer des rôles majeurs dans la sphère publique, bien que dans un registre populaire, sur des sujets relevant des préoccupations politique, économique ou sociale. Internet et davantage les médias sociaux, seraient désormais, dans cette optique, l'outil structurant d'une démocratie participative et délibérative (Trippi, 2008)[2]. On assiste, dès lors, à la naissance d'un nouvel espace politique (Castells, 2001)[3] et à la reconfiguration de l'espace public dans des entités politiques d'un pays où la parole publique était quasiment monopolisée par l'État. Sur un tout autre plan, le terme ***médiacratie***, qui rappelle étymologiquement la notion de pouvoir conduit à envisager plus spécifiquement la suprématie éventuelle des médias sur le politique et la captation par ceux-ci du débat public. Deux aspects surgissent dès lors: la place des médias dans la cité et dans son positionnement par rapport à la sphère politique et le rôle des médias dans le processus de politisation des citoyens, pris individuellement et collectivement.

Si les médias se sont, jusqu'ici, positionnés comme étant le «quatrième pouvoir», la reconfiguration actuelle de l'espace public à la fois médiatique et cybernétique pourrait laisser croire à la constitution d'un cinquième pouvoir (Grallet et al, 2006). Dès lors, émerge un besoin majeur d'analyse des rapports entre médias et politique dans la société contemporaine: d'où notre intervention. Elle apportera au préalable, des éclaircissements sur les concepts: mondialisation, cyberespace et médiacratie qui ont un effet sur le processus sécuritaire. Par la suite, nous allons nous attarder sur la médiacratie cybernétique, avant de mettre en relief médiacratie cybernétique et enjeux sécuritaires.

---

[2] Trippi J., 2008,The Revolution Will Not Be Televised: Democracy, the Internet and the Overthrow of Everything, Harper Collins, New York.

[3] Castells Manuel, 2001, La galaxie Internet, Fayard, Paris.

I - MONDIALISATION ET CYBERESPACE

1 - DE LA MONDIALISATION

Il s'agit d'un des concepts les plus en vogue depuis le milieu des années 90, non seulement dans le milieu des sciences sociales, mais également au sein du grand public. Les définitions de la mondialisation sont nombreuses dans la littérature scientifique, ce qui entraîne une certaine confusion quant à l'utilisation de ce terme. Ainsi, le terme mondialisation est employé de manière peu rigoureuse «comme un mot parmi d'autres pour désigner simplement l'internationalisation plus poussée de l'activité économique s'exprimant par une intégration et une interdépendance accrues des économies nationales» (Thompson, 1999, p.159)[4].

Plusieurs définitions proposées pêchent soit par minimalisme, en réduisant le phénomène à ces manifestations économiques, soit par généralisation excessive en l'associant à tous les changements modernes au sein de la société humaine. Dans le milieu des sciences économiques et du monde des affaires par exemple, on utilise fréquemment le concept de mondialisation pour ne référer qu'à l'accroissement des transactions commerciales et financières transfrontalières. Dans sa définition de la mondialisation, Jean-Luc Ferrandéry (1998, p.3) insiste sur la nature capitaliste de ce concept qui, selon lui, désigne un «mouvement complexe d'ouverture des frontières économiques et de déréglementation, qui permet aux activités économiques capitalistes d'étendre leurs champs d'action à l'ensemble de la planète[5].» Selon une interprétation encore plus restreinte de la mondialisation, celle-ci résulterait d'un ensemble de stratégies économiques résidant dans l'esprit des décideurs, et en particulier des dirigeants d'entreprises privées (Kherdjemil, 1999[6]; Mucchielli, 1998[7]). Ce point de vue est fortement contesté par plusieurs observateurs qui affirment

[4] Thompson et al., 1999, Exacting beauty: Theory, assessment, and treatment of body image disturbance. American Psychological Association. https://doi.org/10.1037/10312-000, P 159

[5] Ferrandéry J.-L., 1998, Le point sur la mondialisation, Paris: Presses universitaires de France, 170 p.

[6] Kherdjemil B., 1998, Mondialisation et dynamiques des territoires, L'Harmattant, Paris.

[7] Mucchielli L., 1998, La découverte du social, La Découverte, Paris.

au contraire que la mondialisation est un processus induit par l'évolution du marché plutôt que le résultat de politiques volontaires (Mittleman, 1996).

Dans les autres disciplines des sciences sociales, le concept de mondialisation est souvent utilisé de manière plus englobante où il représente alors la tendance à «l'interconnexion mondiale croissante» dans pratiquement tous les domaines: économique, culturel, technologique, politique, juridique, militaire, environnemental et social (McGrew, 1997)[8]. Grahame Thompson (1999, p.159) va jusqu'à dire qu'elle fait intervenir «la totalité des phénomènes sociaux contemporains». La principale lacune généralement associée à une interprétation aussi large est qu'elle fournit peu d'outils qui pourraient être utilisés dans une analyse empirique cherchant à spécifier les causes et les conséquences du phénomène de la mondialisation. Les lignes directrices de la mondialisation peuvent, selon Anthony McGrew (1997), se résumer dans les caractéristiques suivantes;

L'interdépendance: par l'effet de l'échange et de la diffusion de l'information, les activités sociales, politiques et économiques transcendent les frontières nationales de telle sorte que les événements, décisions et activités situés à n'importe quel endroit dans le monde peuvent affecter les individus et les communautés en tout point du globe.

L'effacement des frontières nationales: la frontière entre ce qui est local et ce qui est global devient de plus en plus floue. Il est par conséquent plus difficile de distinguer ce qui est «interne» de ce qui est «externe».

Le conflit de souveraineté: l'interdépendance croissante génère de plus en plus de problèmes transnationaux mettant en question la souveraineté nationale. Ces questions ne peuvent être résolues que par la voie du multilatéralisme intergouvernemental.

La complexité systémique»: l'augmentation du nombre d'acteurs et des liens entre eux, entraîne une intensification et une complexification du système mondial et génère une contrainte systémique sur leurs activités et leur autonomie.

[8] McGrew A., 1997,*The transformation of democracy*: *globalization and territorial democracy*, Blackwell Publishers, Cambridge.

Un autre aspect central de la mondialisation qui est généralement reconnu par les chercheurs est celui de la ***compression de l'espace-temps***. Cette expression réfère aux transformations profondes au sein de nos sociétés qui se produisent à un rythme accéléré, se calculant en années plutôt qu'en générations (Mittleman, 1996)[9], ainsi qu'à l'érosion du sens traditionnel des notions d'espace, de territoire et de région, qui semblent réduites à un simple support à l'économie mondiale (Hiernaux-Nicolas, 1999)[10].

Le phénomène peut donc être perçu comme l'unification du monde dont les prémices commencent à se cristalliser autour du 13ème siècle. En voici quelques indicateurs;

1200-1600: des évènements majeurs de l'histoire, amorcent une mise en connexion physique de différentes parties du monde, jusque-là séparées par la géographie: le temps des explorateurs, avec des expéditions telles que la route de la soie, l'expansion de l'Islam vers l'Asie, la «découverte de l'Amérique», la conquête des cinq continents par les puissances impériales européennes;

1870-1914: le décloisonnement du monde se confirme avec notamment l'essor des transports, l'invention du télégraphe, puis du téléphone, des investissements massifs de l'Europe vers les colonies, un vaste mouvement des populations européennes, estimé à 55 millions de personnes qui émigrent de la vieille Europe vers le nouveau monde;

Depuis 1990: il s'est confirmé la mise en place d'une nouvelle configuration du monde, avec comme événements majeurs, la chute du Mur de Berlin et la désintégration de l'Union des Républiques Socialistes Soviétiques (l'URSS) le passage de la Chine à l'économie de marché, la montée en puissance des tigres d'Asie (Corée du Sud, Taïwan, Indonésie). Dans le même espace-temps, l'on a noté l'essor des marchés émergents, symbolisé par les BRICS (Brésil, Russie, Inde, Chine, Afrique du Sud) et les mouvements humains induits, notamment le tourisme. Aux ingrédients

[9] Mittelman J., 1996, *Globalization: critical reflections, Lynne Rienner Publishers,* Australia, 273 p.
[10] Hiernaux-Nicolas D., 1999, *Fondements territoriaux du libéralisme contemporain, Revue Tiers Monde Vol. 40, No. 157, Le libéralisme en questions (janvier-mars 1999), pp. 107-120.*

humains et économiques nécessaires à la consécration (consolidation) de la mondialisation, viendra s'ajouter un élément nouveau, **le Web** (World Wide Web). La toile d'araignée géante, née du fait de l'interconnexion des centaines de millions d'ordinateurs disséminés à travers le monde.

Les progrès des sciences de l'information et de la communication ne sont donc pas en reste dans la variabilité des définitions du terme mondialisation, car du fait du décloisonnement géographique de la planète, de l'existence d'une grande variété de modalités, d'outils de communication et des possibilités d'interactivité, le monde est aujourd'hui à l'image du village planétaire de Marshall McLuhan,»où l'on vivrait dans un même temps, au même rythme et donc dans un même espace»[11]. L'ampleur de l'interconnexion et l'intensité des flux d'information circulant dans l'incommensurable réseau mondial de communication ont donc favorisé la création d'un nouveau continent virtuel: le cyberespace.

2 - DU CYBERESPACE

Aujourd'hui considéré comme le 7e continent, le cyberespace est un réseau informatique couvrant toute la planète, un monde virtuel d'interconnexion au réseau global, de ressources informatiques et des dispositifs fixes et mobiles qui communiquent entre eux. Il apparaît comme un territoire virtuel, un espace à part, sans frontières, qui se veut libre des contraintes du monde physique, avec le *cloud* qui en renforce le caractère irréel. Cette représentation occulte toutefois la complexité d'un espace multidimensionnel, en apparence intangible, mais solidement ancré dans le monde physique, et traversé de conflits géopolitiques bien réels. Le cyberespace est un domaine complexe, comprenant:

Une couche physique qui permet l'interconnexion des ordinateurs, quel que soit le point géographique de l'univers dans lequel ils sont localisés. Cette *première couche «physique»* ou «*matériel*» qui regroupe les appareils d'extrémité (ordinateurs, box de fournisseur d'accès internet, disques durs, carte de crédit, distributeur de billet de banque…) ainsi que les

[11] McLuhan Mashall, 1968, Pour comprendre les médias, Seuil, coll. Points, 404 p. (titre original: (en) Understanding Media: The Extensions of Man, McGraw-Hill, New-York, 1964.)

infrastructures de réseau. Cet ensemble traite l'information et la transmet. Cette couche dépend d'un territoire, sur lequel sont implantés les serveurs ou les fermes de données (Datacenter) ainsi que les câbles et les moyens de transmission terrestre, aérien ou spatial qui permettent leur connexion. Ce territoire a sa législation – donc sa souveraineté.

Une couche logique *ou «logicielle ou* couche service, regroupe les dispositifs de codage et de programmation qu'utilisent les machines. La pensée humaine est transformée en information via des interfaces homme-machine et des protocoles permettant la communication entre les machines au sein d'un réseau, afin qu'elles puissent se transmettre l'information. La couche logique a introduit le cyberespace au sein de la sphère privée des individus et ce de manière permanente. Cela donne aujourd'hui, l'informatique ubiquitaire, en référence au don d'ubiquité, cette faculté extraordinaire, pouvant permettre à un même individu d'être à plusieurs endroits en même temps ou de faire plusieurs choses à la fois. Ce qui était autrefois exceptionnel ne l'est plus aujourd'hui, grâce aux objets connectés en notre possession: le téléphone, les puces, les cartes de crédit, les dispositifs de géolocalisation, etc. C'est dans cette couche qu'on pourrait situer le web, qui lui-même, se décline en différentes dimensions dont voici quelques-unes;

Le Web visible[12]**,** la couche de surface, la partie «visible» de l'iceberg, que les usagers fréquentent au quotidien car accessible par le biais **des navigateurs classiques** (Google Chrome, Internet Explorer et Firefox, Safari, etc.). La couche superficielle du Web représente cependant moins de 5 % du volume total d'Internet.

Le Web profond (Deep Web), partie immergée de l'iceberg, la plus grande partie de la créature, représente environ 90 % de l'Internet. Il abrite un ensemble caché de sites accessibles uniquement par des tunnels spéciaux de navigation.

Le Dark Web, la partie sous l'eau de l'internet, le Web profond, dispose en son sein d'une poche secrète, **le Dark Web**, encore plus difficile d'accès.

[12] Encore appelé Web de surface ou web propre

C'est essentiellement dans ce Web interlope que prospère la cybercriminalité.

Une couche sémantique, *«cognitive» ou «informationnelle»* regroupe les *données ou métadonnées* qui sont transportées par le réseau. Ces métadonnées sont qualifiées de *données de masse.* Elles peuvent permettre de déterminer les goûts des consommateurs et influencer ou favoriser la prise de décision d'achat. Une donnée transporte donc une *information* sur la personne qui la produit. Un ensemble d'informations donne un *message* assimilable à une opinion générale ou collective constituant la dimension informationnelle du réseau. Ainsi le cyberespace considéré comme le 7e continent, doit être appréhendé globalement au travers de cette sédimentation et non uniquement par la seule dimension logicielle.

3 - DE LA MÉDIACRATIE

La médiacratie désigne le pouvoir qu'exercent les médias au sein de la société, soulignant leur influence, en tant que contre-pouvoir, (le 4e pouvoir) face aux pouvoirs exécutif, législatif et judiciaire[13]. Le terme médiacratie peut donc faire successivement référence à:

- à la concentration des médias aux mains de grands groupes capitalistes, et à l'importance que revêt la maîtrise ou le contrôle des moyens de communication par le gouvernement.
- à une connivence entre le pouvoir politique et les médias, conduisant à une certaine forme de «néo-totalitarisme», à la suprématie des médias sur la politique,
- au rôle des médias dans l'élaboration des convictions politiques des citoyens.
- à «l'impact primordial de la télévision, du cinéma, d'Internet et de la publicité sur l'opinion publique, la politique, le marketing, etc.».

Il est important de rappeler que le concept de «médias» renvoie à des réalités distinctes: une technique (la presse): un usage (l'information): des

[13] Les néologismes «vidéocratie», «télécratie» ou «télépopulisme» peuvent être considérés comme des synonymes de «médiacratie».

publics potentiels ou effectifs; une institution (l'entreprise de presse): un genre (le feuilleton). Le concept couvre également l'ensemble des canaux et des supports utilisés pour porter et transmettre un message, notamment par le biais de la presse écrite, de la radio ou de la télévision. Ces médias générés par une seule source, se caractérisent par un mode de transmission unidirectionnel et non alternatif, de l'émetteur vers le récepteur. Ils sont, depuis la révolution des TIC catégorisés comme médias traditionnels. En effet, les technologies du Web ont engendré des médias d'un type nouveau: simples, accessibles et privilégiant le mode participatif et donc l'interaction. Ainsi, les blogs, wiki et autres plateformes de partage, générés de manière collaborative et interactive entre groupes d'internautes interagissant à la fois comme émetteur-récepteur-réémetteur, sont qualifiés de médias sociaux. Le terme «social», quant à lui, exprime l'existence de relations entre individus ou groupes d'individus partageant des modes de vie, des normes et des valeurs qui, de par leur interaction, sont vecteurs d'influences réciproques, favorisant la formation de groupes ou de communautés. Cette reconfiguration des médias due aux TIC, nous amène donc à repenser la médiacratie à l'ère du numérique.

II - GENEALOGIE DE LA MEDIACRATIE CYBERNETIQUE

1 - LA CYBERNÉTIQUE COMME FONDEMENT THÉORIQUE

Emanation de la cybernétique, science émergente déjà définie en 1834 par André-Marie Ampère comme «la science du gouvernement des hommes». La cybernétique a été redéfinie de manière plus explicite par Norbert Wiener comme «la science de la communication et du contrôle chez l'animal et la machine. Cette deuxième définition postule qu'une seule et même discipline puisse s'appliquer aux machines et aux animaux (donc par extension aux humains). Elle met sur un pied d'égalité la communication et le contrôle.

Sous cet angle, la cybernétique, peut être vue comme une science de

l'action, fondée sur l'étude des processus de commande et de communication chez les êtres vivants, dans les machines et dans les systèmes sociologiques et économiques. La cybernétique est donc une «techno-science» du contrôle des systèmes par la gestion des flux de données et informations. A ce titre, elle constitue une véritable révolution épistémologique et un profond changement de paradigme par rapport au cartésianisme prédominant dans la science classique.

Dans sa dimension sociale, la cybernétique a donné naissance à l'Internet, le plus vaste et le plus sophistiqué réseau de communication dans le monde. Ses applications sont multiples: ordinateurs, smartphones, robots, intelligence artificielle, automatismes industriels, internet, etc. Autant dire que la cybernétique a colonisé la quasi-totalité des sciences et techniques. Mais ses effets ne se cantonnent pas aux secteurs technologiques. Ses principes et ses modes de pensées s'étendent désormais à de nombreux secteurs des sciences sociales et de la vie politique. La cybernétique met donc en évidence;

Le rapport d'un système avec son environnement. Le système échange des informations avec son environnement qu'il est capable de transformer.

Le concept de «boite noire». Il n'est pas toujours nécessaire de comprendre les rouages d'un système. Il suffit de comprendre la façon dont il transforme des inputs en outputs, à l'exemple de :

- **l'émetteur**, qui agit sur l'environnement, donc envoie de l'information, sorte de porte de sortie, et;
- du **récepteur**, qui en intègre depuis l'environnement, donc capte les informations, comme une porte d'entrée de la boîte noire;
- du **flux d'information**: ce qui est transmis, donc envoyé et effectivement reçu, autrement dit l'information efficace dans les systèmes de communication;
- de la rétroaction (**feedback**): c'est l'information en retour de l'état. Un élément essentiel de la **communication digitale** de nos jours.

L'importance des flux d'informations. Les systèmes et leurs composants captent, transforment et émettent des flux d'information que

l'on doit connaître / paramétrer pour contrôler le système.

Associer médiacratie et cybernétique pourrait sembler une opération périlleuse au regard de l'impact des deux notions sur le contrôle d'environnement aujourd'hui. Il s'agit, en fait, de mettre en relation cybernétique, société, information, pouvoir et émergence d'un agir collectif. La cybernétique fait revivre la médiacratie, mais la médiacratie est une conséquence de la cybernétique.

2 - DE LA MÉDIACRATIE CYBERNÉTIQUE

Pour M. GURRY (2019)[14], *après l'invention de l'écriture, de l'alphabet, de l'imprimerie et l'arrivée des médias de masse de l'âge industriel, le monde est entré dans une cinquième vague*[15] *portée par l'apparition du web en 1990*. Le changement de paradigme né de l'Internet, en donnant la parole à tout le monde, chacun exprimant ses intérêts et ses émotions du moment, anéantit l'idée d'une société organisée selon une hiérarchie des savoir et des positions, dans le gouvernement, les entreprises, les universités, etc. Le *Digital Age*, a donc entraîné ce que Gurry considère comme la révolte du public, et partant, la reconfiguration de l'espace public. En effet, la Web culture et le sentiment de puissance que procurent les médias sociaux, ont pris le relais des médias classiques. Le Web a fait éclater les frontières entre paroles d'autorité et paroles profanes: entre les propos des journalistes reconnus et des experts déversés dans la presse écrite et la télévision, d'un côté, et paroles d'acteurs concernés ou engagés, d'amateurs éclairés ou de penseurs du dimanche, qui meublent les plateaux de télévision dans notre pays. L'évolution de la médiacratie serait donc étroitement liée au cyberespace et à ses différentes dimensions.

À n'en point douter, le développement de la cybernétique a favorisé l'élargissement de la sphère publique à de nouveaux acteurs, qui se positionnent radicalement contre le centre de la société, contre les pouvoirs organisés, campent sur un refus absolu de l'ordre établi et fonctionnent selon un élan unilatéral, visant à provoquer un maximum de nuisance. C'est

[14] M. GURRY, *The revolt of the public and the crisis of authority in the new millenium*, Stripe Press, 2018, 449 p. (3 juin 2019)

[15] Par allusion à *the 5th wawe*, film américain de science-fiction, réalisé par Jonathan Blakeson, sorti en

désormais le public qui a le contrôle des moyens de communication. Il sert à profusion: le propos partisan, l'état d'âme, l'exaltation, l'invective, la dénonciation, le ricanement méchant, l'affirmation péremptoire, la rumeur, l'insinuation. Toute erreur, tout événement peut amener un public connecté dans la rue et n'importe quelle étincelle est susceptible de déstabiliser n'importe quel système politique, n'importe quand et n'importe où. Si les médias se sont jusqu'ici positionnés comme étant le «quatrième pouvoir», la reconfiguration actuelle de l'espace public à la fois cybernétique et médiatique pourrait laisser croire à la constitution d'un cinquième pouvoir (Grallet et al, 2006).

En effet, depuis l'avènement de l'informatique et plus encore depuis le déploiement du réseau Internet, les promesses de réinvention démocratique se sont multipliées: horizontalité, vitesse, participation seraient devenues les maîtres mots d'un nouvel agir public mondialisé à travers l'information amplement relayée par les médias. Dans son ouvrage ***Le pouvoir des médias*** (2017), Grégory Derville s'intéresse au pouvoir des médias ainsi qu'aux rapports entre le champ politique et les médias. Les sociétés occidentales et africaines ont connu au cours des dernières décennies la montée en puissance des médias. Celle-ci se manifeste par l'engouement des ménages pour l'acquisition de nouveaux appareils de communication, par la forte consommation des programmes télévisés ainsi que par la hausse de fréquentation des sites Web et des réseaux numériques. Ces bouleversements ont touché également le champ politique, qui a dû adopter des techniques et des modes de fonctionnement particuliers dictés souvent par les médias, les instituts de sondage et les conseillers en communication. Les médias d'information contribuent à augmenter le niveau d'information du public, ils peuvent modifier leur stock de connaissances, ils peuvent influencer leurs visions du monde, leurs raisonnements. Toutefois, ces mêmes médias sont capables d'orienter l'attention du public sur certains enjeux précis et exercent, de ce fait, une hiérarchisation des priorités: il s'agit du concept d'agenda-setting proposé par Maxwell McCombs et Donald Shaw en 1972[16]. En s'exposant aux médias d'information, les individus sont «moins susceptibles

[16] Maxwell McCombs et Donald Shaw, 1972, "*The Agenda-Setting Function of Mass Media*" in The Public Opinion Quarterly Vol. 36, No. 2 (Summer, 1972), pp. 176-187 (12 pages), Oxford University Press

de mettre en marche les mécanismes de défense décrits par le paradigme des effets limités» (Katz, 1989: 80). Les messages médiatiques véhiculés sont donc plus influents, car ils touchent l'aspect cognitif et peuvent même exercer une influence sur le plan évaluatif, voire conatif. La théorie de l'agenda-setting a le mérite de rappeler que l'influence des médias dépasse leur fonction de transmetteur d'information, mais réside dans leur capacité à structurer les préoccupations et les connaissances du public. À défaut de dire aux citoyens ce qu'il faut penser, les médias sont en mesure de dire au public «à quoi il faut penser», notamment en médiatisant certains problèmes plutôt que d'autres. Après l'effet d'agenda-setting et l'effet de cadrage, un autre mécanisme mis en évidence par Shanto Iyengar (cadrage) et Donald R. Kinder (1987) démontre l'influence des médias sur le jugement du public: il s'agit de l'effet d'amorçage qui consiste à évaluer les partis et les acteurs politiques à partir de la position qu'ils prennent par rapport au thème en question.

Le pouvoir des médias a en outre accentué les disparités entre les groupes sociaux et culturels, comme l'ont si bien formulé Philip Tichenor, George Donohue et Clarice Olien à travers le concept de *knowledge gap* en 1970. En effet, les personnes plus favorisées sur le plan socioculturel ont tendance à être mieux équipées en technologies de communication, elles sont mieux informées, elles sont plus attentives aux informations qu'elles reçoivent, plus critiques à l'égard des médias que ne le sont les personnes issues des couches défavorisées de la population. Par ailleurs, la médiatisation exerce une influence sur la vie politique sur plusieurs plans, d'abord sur la sélection du personnel politique. Auparavant, l'exercice d'une activité politique nationale exigeait d'avoir un certain nombre de ressources partisanes et parlementaires. Avec la surmédiatisation, cette condition n'est plus suffisante pour être un bon acteur politique. Il faut désormais savoir séduire un public plus vaste, plus hétérogène, principalement formé par des individus peu ou pas politisés. Cela suppose de maîtriser des qualités spécifiques, des savoir-faire et des savoir-être. Il ne suffit plus d'être intègre, compétent et honnête, il faut surtout savoir se mettre en scène et surligner ces qualités.

La médiatisation tend ainsi à susciter chez les acteurs politiques, une forte focalisation sur le court terme. Les médias exercent un impact important sur l'activité interne du champ politique, et en particulier sur l'activité

gouvernementale, car ils font émerger des dossiers brûlants tout en appelant une réaction rapide. Ils peuvent influencer ou bousculer l'agenda politique, et surtout l'agenda gouvernemental. Les acteurs politiques doivent ainsi en permanence mettre en scène le fruit de leur travail pour qu'il soit visible pour les journalistes et les citoyens. Ils essayent à longueur d'année, par leurs déclarations comme par leurs décisions, d'occuper l'espace médiatique, en réagissant au plus vite au moindre événement sur lequel il est possible de rebondir, en s'engouffrant dans la moindre fenêtre médiatique.

De plus en plus, à l'ère des médias et des Technologies de la Communication, l'action politique est structurée selon un impératif de visibilité et de spectacularisation en vue de capter l'approbation des médias et de l'opinion publique. Le processus de médiatisation de la politique a également entraîné des transformations dans le discours des professionnels de la politique. En effet, le développement des médias de masse a poussé les acteurs politiques à remplacer le modèle de discours classique de type magistral par des formes de discours plus souples, plus fluides et plus concrètes. Une telle évolution tient à plusieurs facteurs, d'abord d'ordre technologique: la radio et la télévision constituent des supports de communication différents de la presse écrite puisque le locuteur peut être vu et entendu. Dans un contexte de prolifération des sources d'information et de distraction, il devient de plus en plus difficile de capter l'attention du public. Les professionnels de la politique doivent donc en permanence, développer des discours avec un contenu extralinguistique riche, en théâtralisant leur exposition médiatique par la posture du corps, la mise vestimentaire, les gestes, les mimiques, les regards, etc.

Les technologies de l'information et de la communication, en particulier Internet, tendent à accroître la diffusion de ces formes de participation ponctuelles et limitées au détriment des formes plus traditionnelles. Internet propose des modalités de participation (cyber manifestations, pétitions en ligne, participation à un réseau social de parti politique) moins contraignantes avec un coût d'entrée et de sortie limité et un gain de temps. Petit à petit, le Web s'est imposé comme un espace virtuel de mobilisation. En outre, la montée en puissance de ces nouveaux médias a influencé les processus de mobilisation collective. Les médias sont de plus en plus instrumentalisés par

les groupes en lutte pour mobiliser les sympathisants, pour transmettre les informations et les mots d'ordre entre les militants et pour structurer leur organisation (à l'interne).

III - MANIFESTATIONS ET ENJEUX SECURITAIRES LIES A LA MEDIACRATIE CYBERNETIQUE

Les changements incessants dans la recomposition permanente de l'espace public depuis l'avènement de l'Internet ubiquitaire. En effet, l'essor des data sciences et donc de la cybernétique tendent à convaincre l'opinion d'être désormais productrice de l'information, passant du rôle d'acteur passif qui hier subissait l'information à celui d'acteur actif qui fait et défait l'information. En Occident plus que partout ailleurs, le discours du pouvoir occupe désormais une place réduite dans la sphère de l'information, avec des conséquences qui semblent irréversibles. L'on assiste alors, à l'échelle planétaire, à des manifestations telles que: la désacralisation du discours officiel au profit de la parole errante: la défiance de l'autorité: l'accaparement de la scène médiatique par des acteurs autoproclamés «influenceurs, lanceurs d'alertes»: la divulgation et prolifération de fausses nouvelles, diffamation, chantage, etc. En somme, les réseaux pratiquent un égalitarisme fanatique, sans craindre d'engendrer des dysfonctionnements sociaux majeurs. Une seule personne, un seul événement, une seule alerte puissamment répercutée sont capables d'entrainer des milliers d'individus dans un mouvement d'opinion viral. Quelques exemples bien connus de mouvements survenus en divers lieux géographiques, mais ayant pour dénominateur commun, la coordination des opérations à partir des médias sociaux et des sites web;

Los Indignados: mouvement inspiré de «Indignez-vous», un essai de Stephan Hessel, publié en 2010. Les actions initiées en Espagne, le 15 mai 2011, rassemblant des centaines de milliers de manifestants pour des marches ou des campements pacifiques. Ce mouvement qui ne faiblit qu'en 2015 en inspirera d'autres à travers le monde.

Occupy Wall Street: mouvement de contestation pacifique à partir du 17 septembre 2011 dans le quartier de la Bourse à New York, dans le but de dénoncer les abus du capitalisme financier. Les semaines suivantes, le mouvement s'étendra à 45 Etats américains et à 28 pays étrangers.

La place Tahrir est devenue le symbole de la révolution égyptienne. Divers mouvements appellent à manifester dès le 25 janvier 2011 pour une journée de revendications politiques baptisée «journée de la colère». Ces manifestations qui chaque jour gagnent en ampleur, aboutiront le 10 février 2011 à la chute du Président Hosni Moubarak.

Les Gilets Jaunes: le mouvement de protestation apparu en France en 2018 s'inscrit dans le même registre que les exemples ci-dessus évoqués.

Tous ces événements ont soudain mis en lumière, le caractère peu anodin des tweets, sms et autres flashs instantanés, construits, «co-construits», nourris en temps réel par la communauté numérique, puis lâchés dans l'agora, «le village planétaire» qu'est le monde d'aujourd'hui.

Au-delà de ces mouvements désormais gravés dans l'histoire du monde contemporain, il convient également de relever l'encensement des lanceurs d'alerte, qui incarnent l'esprit[17] de la médiacratie cybernétique. On citera entre autres: en 2013, Edward Snowden révélant des secrets sur le système de surveillance de la NSA: Julian Assange publiant en 2010, via Wikileaks, des documents américains classés secret Défense.

1 - QUELQUES MANIFESTATIONS DE LA MÉDIACRATIE CYBERNÉTIQUE AU CAMEROUN

La médiacratie cybernétique au Cameroun se manifeste à travers la construction d'un débat démocratique caractérisé par la réappropriation politique locale de l'espace public numérique, la réinvention de la citoyenneté des individus, la prolifération des Fake news et des phénomènes tels que le bashing[18] et l'organisation de manifestations anti-

[17] Monique Dagnaud,¨ Réguler Internet? Même pas en rêve¨. In *Wired* 10 novembre 2019

[18] Le *bashing* est le fait de dénigrer collectivement une personne ou un sujet, se retrouvant partout sur internet. A chaque nouvelle polémique, lynchages, insultes sont systématiquement au rendez-vous.

gouvernementales. Le premier élément est relatif à l'implication des camerounais vivants à l'étranger dans les affaires politiques. L'on note en effet une transformation des espaces et la fluidification des rapports sociaux et politiques entre les Camerounais émigrés, leurs compatriotes vivant au Cameroun et leur État d'origine, avec en prime une tendance à la promotion du non – Etat dans les médias classiques et les médias sociaux en l'occurrence. Les sites de médias camerounais, de même que les sites communautaires, ne permettent pas seulement de diffuser des articles d'opinions, ils permettent aussi aux internautes camerounais de réagir face à l'actualité politique locale ou globale, et de contre-réagir en publiant des articles collectifs ou individuels. En revanche, si les blogs s'apparentent encore à des espaces destinés au stockage des informations se rapportant aux activités des membres de la communauté diasporique, les sites communautaires ainsi que les «cyberjournaux» s'illustrent comme des plates-formes d'échanges d'opinions avec les membres de la communauté politique et la promotion du «Breaking News». Il n'est donc pas surprenant de voir dans les médias sociaux, des informations et opinions qui diffèrent totalement de la réalité. Il faut aussi relever qu'au Cameroun, la création de sites web d'information ou des blogs n'est pour le moment soumise à aucune règle.

Dans l'environnement local, l'affaire Koumatekel, cette dame éventrée dans la cour de l'Hopital Laquintinie de Douala reste, à travers l'ampleur que les médias sociaux ont donnée à l'événement, un exemple typique de manifestation de la médiacratie cybernétique au Cameroun :

- face aux caméras-téléphones de la foule, qui filment, commentent et diffusent, depuis la cour de l'hôpital, la famille de la défunte impute la responsabilité des décès de la mère et des bébés au corps médical accusé de négligence;
- dans le brouhaha qui se déchaîne alors, les arguments du personnel hospitalier tentant de convaincre l'opinion que la patiente était déjà décédée à son arrivée à l'hôpital, resteront inaudibles;
- l'avis médical tentant d'expliquer que la vie du fœtus, in utero est liée à celle de la maman peine à convaincre;

Même les points de presse du gouvernement prenant appui sur la

communication publique n'obtiendront pas l'effet escompté.

Tant au plan local qu'à l'étranger, l'affaire secoue l'opinion et entraine des prises de position tranchées et une grande variété d'actions: manifestations des partis politiques d'opposition, d'organisations et d'associations diverses, de la diaspora camerounaise, collecte de fonds supposément destinés à la famille; critiques virulentes de l'Etat et du système de santé. Dans ce brouhaha, tout ce qui compte et fait foi, c'est ce qui se dit sur Internet.

2 - ENJEUX SÉCURITAIRES

Avant toute chose, il est important de procéder à la clarification des concepts de cybercriminalité, cyber sécurité et cybercriminels, qui ne peuvent être séparées dans un environnement numérique interconnecté. La cybercriminalité désigne une activité illégale commise à l'aide d'ordinateurs ou d'Internet, notamment: les activités terroristes l'espionnage, le piratage illégal de systèmes informatiques, les infractions liées au contenu, le vol et la manipulation de données, le cyber harcèlement, etc. Tandis que la cyber sécurité ou la gestion de la cybercriminalité, désigne l'ensemble des outils, politiques, concepts de sécurité, mesures de protection, lignes directrices, approches de gestion des risques, actions, formations, meilleures pratiques, assurances et technologies qui peuvent être utilisés pour protéger le cyber environnement et les biens des organisations et des utilisateurs. Les cybercriminels quant à eux, sont des individus, aussi bien que des groupes organisés qui se servent des techniques de pointe, des systèmes de télécommunication et des applications pour exécuter des cyber attaques destinées au monde physique, à travers l'utilisation des malware, logiciels hostiles et malveillants, sous forme de virus informatique, vers, cheval de Troie, ransomware, spyware, adware, scareware, enregistreurs de frappe de clavier, etc.

Le 7^{e} continent dispose donc d'un réseau informatique couvrant toute la planète. Un monde virtuel d'interconnexion au réseau global, de ressources informatiques et des dispositifs fixes et mobiles qui communiquent entre eux. Le nouveau continent contrôle des moteurs de

recherche capables d'interroger en millisecondes des bases de données rassemblant tout le savoir humain. Des virus informatiques fabriqués dans des laboratoires militaires, puis détournés par des pirates surdoués. Des sociétés informatiques plus puissantes que des États. Des banques fonctionnant uniquement en ligne. Des menaces terroristes réalisées par l'intermédiaire de communications électroniques. Des univers de jeux regroupant des populations entières. Des drones capables d'espionner et de tuer n'importe qui, n'importe où. Des machines contrôlées grâce à des interfaces visuelles ou des électrodes collées sur le crâne. Des puces implantées sous la peau ou dans le cerveau. Des outils permettant le pistage intégral d'un individu grâce aux *«traces numériques hétérogènes»* qu'il laisse partout à son insu.

Cet univers glauque à souhait, est peuplé d'une foule hétéroclite, tant dans sa composition, dans ses intentions que dans son fonctionnement dont la vision politique se situe à mi-chemin entre une utopie libertaire et anarchiste. Gustave Le Bon[19], décrit la foule comme une «âme collective» avec laquelle les individus qui la composent entrent en fusion, une sorte de «cerveau général». La «foule numérique», née de la cybernétique est aujourd'hui composée des hackeurs sans foi ni loi, des bandes de «*mercenaires, farceurs, nihilistes, techno fétichistes»,* souvent malveillants, qui pénètrent des serveurs à distance pour voler ou détruire des données. Ils peuvent organiser des actions clandestines pour perturber un réseau, se cacher, emprunter des identités et utiliser de nombreuses techniques pour dissimuler leurs agissements dans la masse des données qui défilent.

Les foules numériques ont la capacité d'abolir les frontières et de générer une adhésion massive et immédiate; il suffit de cliquer sur un bouton pour exprimer un sentiment positif ou négatif, pour soutenir ou dénoncer une cause. La supériorité numérique qui a le pouvoir de **déresponsabiliser l'individu**, va de pair avec la **contagion émotionnelle.** *Dans les foules, les idées, les sentiments, les émotions, les croyances possèdent un pouvoir contagieux aussi intense que celui des microbes[20]».*

[19] Gustave Le Bon, *Psychologie des foules*, Editions Echo Library

[20] Du fait de l'instantanéité et de l'omniprésence de l'information qui empêchent souvent le recul nécessaire à la réflexion on parle de vidéo ou de publications virales.

CONCLUSION: DE LA NÉCESSITÉ DE REPENSER L'ESPACE PUBLIC CAMEROUNAIS

Internet a favorisé la création d'un espace numérique sans frontières géographiques, accessible à tous par une grande diversité d'applications et d'équipements au caractère convivial. Tout usager d'internet ou du téléphone mobile, à travers la rédaction et l'envoi de mails, de tweets ou de sms, est potentiellement émetteur et récepteur d'informations. Le citoyen du monde numérique se promène, cherche et dans l'endroit où il se trouve, à se saisir de l'information ou ce qu'il considère comme tel et la lâcher dans le cyberespace, sans aucun filtre. Les échanges entre les acteurs de la scène numérique, dépourvus d'identité, d'ancrage professionnel et de responsabilité, disséminés à travers le monde contribuent largement à l'accélération de l'instantanéité, à la propagation rapide et à l'amplification de l'information, qu'elle soit à caractère social, politique ou commercial. Internet, dans l'usage qu'en font les idéologues et les foules, apparaît comme une expression errante, un avatar technologique dont des «prolétaires intellectuels» désorientés, se servent pour manipuler, relayer des ragots et régler des comptes. L'idéologie du tout numérique aboutit d'après le philosophe Nkolo Foe[21], *«au triomphe de l'esprit grégaire et à l'avènement d'un individu vide, sans esprit critique».*

En étant au centre, l'espace public médiatique tend à évacuer le politique ou à le permuter. Ainsi, on risque de nourrir l'illusion technicienne selon laquelle, par la médiatisation, la société sera transparente, entièrement visible, sans secret et compréhensible. La médiatisation tend (concourt) à absorber, délégitimer ou occulter les autres formes de médiation. L'espace public, à l'instar du politique, prend racine dans une nation, un espace circonscrit par l'État. Il constitue un lieu de communication de la société avec elle-même. Or, il faut prendre en compte la dialectique qui se noue et les échanges qui ont lieu entre les espaces publics nationaux des diverses sociétés (Ferry, 1989: 20). Dans cette dialectique du national et de

[21] Le Professeur Nkolo Foe, philosophe, enseignant de l'Université de Yaoundé I. Interview accordée au quotidien Le Jour, n°2155 du 31 mars 2016, suite à l'affaire Koumatekel.

l'international, l'espace public est saisi comme un dépassement du cadre de l'État-nation dans la mesure où il permet une communication entre les sociétés par l'échange de représentations. Les médias de masse, en tant que vecteurs de communication, ne portent pas en eux une «vision» de la société, malgré ce que sous-tend le déterminisme technologique de la perspective Mcluhanienne, soit le postulat selon lequel les technologies, tout en étant une projection de ce qu'est l'être humain physiquement et intellectuellement, influencent les facultés et les capacités humaines de même que la société entière. La représentation de la société dans les médias ne découle pas non plus d'une simple manipulation idéologique (dans les pays démocratiques). En raison de leur influence symbolique et de la place centrale qu'occupe la «médiation médiatisée», les médias participent au mouvement de production et reproduction de la société: ils le font en objectivant un espace public qui tend, par sa massification même, à représenter la totalité. Le travail symbolique des médias concerne ainsi la représentation du lien social dans la mesure où ils mettent en forme et en sens la société dont ils font partie. Cette représentation médiatique doit être comprise au regard de la régulation politique mise en œuvre par chaque forme de l'État qui, elle-même, sous-tend une représentation singulière de l'univers des rapports sociaux et du rapport de l'individu à la totalité.

L'espace public, tel que vu par Jurgen Habermas[22], dans ses recherches initiales sur la question en 1962, relève définitivement du passé. L'espace public était le lieu, physique ou symbolique, dans lequel les idées circulaient jadis et où elles étaient discutées de manière rationnelle afin de les cristalliser en opinion publique. Dans cet espace public légitime, les grands médias, faiseurs d'opinion et facilitateurs des débats, définissaient les contenus dignes d'être publicisés, les prises de parole «*médiatiquement acceptables»* et d'autres qui en étaient systématiquement écartées[23]. Il convient donc de considérer l'espace public actuel comme une scène médiatique et dialogique de visibilité politique. L'espace médiatisé que mettent en œuvre les médias de masse est public dans le sens arendtien du

[22] Jurgen Habermas, *L'Espace public* (1962), traduit en français

[23] Zineb Benrahhal Serghini et Céline Matuszak (2009) *Revisiting Habermas's Model of the Public Sphere*

terme: il rend visible le politique, le vivre-ensemble, et le monde commun, comme repère d'appartenance. Ils mettent en scène la parole politique, foncièrement argumentative et dialogique, par leur objectivation et reconstruction du discours originel. L'espace public se redéfinirait par le passage d'un espace public politique à un espace public circonscrit à la question sociale: le social et non plus le politique, seraient l'objet de l'espace public. Dans cet environnement caractérisé par la médiacratie cybernétique, le social prendrait donc le dessus sur les questions politiques, dans le but de favoriser le projet de vivre-ensemble.

A laisser prospérer sans régulation, sans règlementation, la jungle installée par l'informatique ubiquitaire, ne risque-t-on pas de transformer Internet, une des plus grandes inventions humaines en un pharmakon, cet élixir à la fois, remède et poison, puissance curative dans la mesure et puissance destructrice dans la démesure ?

REFERENCES BIBLIOGRAPHIQUES

1 **Arendt H**., 1958, *Condition de l'homme moderne*, trad. de l'américain par G. Fradier, Paris, Éd. Pocket, 2002.

2 **Ballarini L**., 2016, «Relire Habermas: retour sur un concept-piège», *Publics en question*.

3 **Boucheron P**., Offenstadt N., dirs, 2011, *L'Espace public au Moyen Âge. Débats autour de Jürgen Habermas*, Paris, Presses universitaires de France.

4 **Calhoun C.,** (dir.) (1992), *Habermas and the Public Sphere*, Cambridge, MIT Press, 498 p.

5 **Cardon D., Granjon F**., 2010, *Médiactivistes*, Paris, Presses de Sciences Po, 2013.

6 **Chambat P.,** (1995), Espace public, espace privé: le rôle de la médiation technique, in Pailliart I. (dir) (1995), L'espace public et l'emprise de la communication, Grenoble, Ellug, pp. 65-73.

7 **Charaudeau P.,** (1997), Le discours d'information médiatique: la

construction du miroir social, Paris, Nathan, INA, 286 p.

8 **Dahlgren P**., 2000, «L'espace public et l'internet. Structure, espace et communication», *Réseaux*, vol. 18, 100, pp. 157-186.

9 **Elias N**., 1987, *La Société des individus*, trad. de l'allemand par J. Etoré, Paris, Éd. Pocket, 1997.

10 **François B. et Neveu E.**(dir.)**,** (1999), Espaces publics mosaïques. Acteurs, arènes et rhétoriques des débats publics contemporains, Rennes, Presses Universitaires de Rennes, 322 p.

11 **Fraser N**., 1992, «Repenser la sphère publique: une contribution à la critique de la démocratie telle qu'elle existe réellement», *Hermès*, 31, pp. 125-156, 2001.

12 **George E.,** (2001), *Relecture du concept d'espace public à l'heure de l'Internet*, in Actes du XII[e] Congrès national des sciences de l'information et de la communication, Unesco (Paris), pp. 23-31.

13 **Gustave Le Bon***, Psychologie des foules,* Editions Echo Library

14 **Habermas J.,** (1993), L'espace public: Archéologie de la publicité comme dimension constitutive de la société bourgeoise, Paris, Payot, 324 p.

15 **Martin G.,** *The revolt of the public and the crisis of authority in the new millenium*, Stripe Press, 2018, 449 p. (3 juin 2019).

16 **M. McCombs et Donald S.**, 1972, "*The Agenda-Setting Function of Mass Media*" in The Public Opinion Quarterly Vol. 36, No. 2 (Summer, 1972), pp. 176-187 (12 pages), Oxford University Press.

17 **Mercier A. et Nathalie P. C.**, «Mutations du journalisme à l'ère du numérique: un état des travaux», *Revue française des sciences de l'information et de la communication*, Revue en ligne, juillet 2012.

18 **Miège B**., 1995, «L'espace public: perpétué, élargi et fragmenté», pp. 163-175, *in*: Pailliart I., dir. *L'Espace public et l'emprise de la communication*, Grenoble, Éd. littéraires et linguistiques de l'Université de Grenoble.Monique

Dagnaud, Réguler Internet? Même pas en rêve. In *Wired* 10 novembre 2019.

19 **Olivier T.**, «Le "journalisme citoyen" en ligne: un public réifié ?», *Hermès*, n° 47, 2007, pp. 115-122.

20 **Alice N. M.**, Les usages des médias sociaux, *Heuristique*, vol 1, N°2 2013, pp 317-335.

21 **Ruellan D**., 2008, «Garder les pieds sur terre», *Médiamorphoses*, 24, p. 46-50.

22 **Ruellan D**., «Penser le journalisme citoyen», *M@rsouin*, 2007, http://marsouin.org.

23 **Tetu J.-F.,** 2008, «Du "public journalism" au "journalisme citoyen"«, *Questions de communication*, n°13, p. 71-88.

24 **Olivier T.**, «Le "journalisme citoyen" en ligne: un public réifié ?», *Hermès*, n° 47, 2007, pp. 115-122.

25 **Wolton D.,** (1992), *Les contradictions de l'espace public médiatisé*, in Hermès n°10, pp. 95-114.

26 - (1997), *Penser la communication*, Paris, Flammarion, 401 p.

27 -(2000), *Internet et après. Pour une théorie critique des nouveaux médias*, Paris, Flammarion, 240 p.

28 **Zineb B. S. et Céline M., (2009)** *Revisiting Habermas's Model of the Public Sphere.*

LE CYBERESPACE: ENJEUX ET DEFIS A L'ERE DE LA MONDIALISATION

Prosper DJOURSOURBOU PAGOU
Directeur du Computer incident response team en charge de la veille sécuritaire du cyberespace camerounais, ANTIC

RESUME

Après les trois (03) révolutions industrielles qu'a connu le monde et au vu des bouleversements sur les plans socio-économique et culturel impulsés par les Technologies de l'Information et de la Communication (TIC), les experts s'accordent à dire qu'Internet et le cyberespace constituent la quatrième révolution industrielle. Pour tenter de décliner les enjeux et défis inhérents à ces technologies, le présent article a employé une démarche en trois (03) étapes. Dans la première partie, l'écosystème des TIC a été présenté ainsi que les atouts qu'elles recèlent notamment sur les plans socio-économiques. Dans la deuxième partie, le phénomène de la cybercriminalité a été présenté avec notamment les modus-operandi des cybercrimes majeurs et les stratégies employées par les Etats pour y faire face. Dans la troisième partie, fort des atouts et des menaces que peuvent comporter le cyberespace, il a été démontré que ce nouvel espace pouvait constituer s'il était maitrisé, des leviers importants de soft et hard power et par ricochet impacter l'échiquier géopolitique mondial.

INTRODUCTION

Les Technologies de l'Information et de la Communication, grâce à leur transversalité et à leur faculté à optimiser les processus et à faciliter les communications, se sont imposées dans tous les secteurs d'activité notamment la santé, l'éducation, l'industrie et même la gouvernance. Bien que cette mouvance ne soit pas uniforme dans toutes les parties du globe puisqu'il est de notoriété publique que certaines régions notamment l'Afrique subsaharienne sont victimes de la fracture numérique, leur impact est bel et bien visible et perceptible tant sur le plan social que sur le plan économique. De même, leur nature intrinsèque fortement maillée en a fait un catalyseur important de la mondialisation qui introduit une nouvelle forme de conflictualité en marge de laquelle les Etats doivent interagir pour préserver leurs intérêts. Il convient de relever que la baisse des coûts d'accès aux terminaux et à l'Internet combiné au fort maillage des cyberespaces et au développement des technologies de cryptage et d'anonymat ont fait de cet espace un environnement idéal pour la prolifération des menaces asymétriques. Dès lors, comment les Etats doivent-il agir pour capitaliser les atouts du cyberespace pour leur développement et leur rayonnement à l'International tout en mitigeant les risques inhérents à l'usage de ces technologies. Le présent article se propose de répondre à cette question en permettant d'une part d'évaluer au travers d'indicateurs mesurables l'impact du cyberespace sur les plans socio-économiques et d'autre part, de présenter les contours de la cybercriminalité, les stratagèmes pour y faire face et enfin analyser l'impact potentiel de ce nouvel espace dans les rapports de force qui régissent les relations internationales.

I - LES TIC COMME LÉVIER DE DÉVELOPPEMENT

A - PRÉSENTATION DE L'ÉCOSYSTÈME DES TIC

Les Technologies de l'Information et de la Communication désignent généralement l'ensemble d'outils et de ressources technologiques permettant de transmettre, enregistrer, créer, partager ou échanger des informations, notamment les ordinateurs, l'internet (sites Web, blogs et messagerie électronique), les technologies et appareils de diffusion en direct (radio, télévision et diffusion sur l'internet) et en différé (podcast, lecteurs audio et vidéo et supports d'enregistrement) et la téléphonie (fixe ou mobile, satellite, visioconférence, etc.)[1].

Leur naissance remonte au 18ème siècle avec l'invention de la télégraphie et va s'accélérer avec l'invention des transistors en 1948 qui va engendrer la prolifération des circuits imprimés sur lesquels reposent les composants actuels de ces technologies permettant d'atteindre des performances gigantesques en termes de vitesse de traitement et de transmission des données. Au fil des années, vu leur popularité, les TIC ont évolué du simple rang de technologie pour constituer une économie à part entière dénommée économie numérique. Les acteurs de cette économie peuvent être regroupés en quatre (04) principales catégories;

Les producteurs de *hardware*: Cette catégorie regroupe les entreprises qui conçoivent et fabriquent les actifs informatique matériels, des composants les plus élémentaires (transistors, microprocesseur, etc) aux équipements (ordinateur, tablette, téléphone, routeur, etc). Parmi ces entreprises, l'on peut citer Hewlet Packard, Dell, CISCO, SAMSUNG, etc.;

Les éditeurs de *software*: Cette catégorie regroupe les entreprises qui conçoivent et éditent les actifs informatiques immatériels appelées communément «logiciel». Parmi ces entreprises, l'on peut citer MICROSOFT, VMWARE, ADOBE;

[1] UNESCO-Institut statistique, «Glossaire FR», Technologies de l'Information et de la Communication (TIC), http://uis.unesco.org/fr/glossary-term/technologies-de-linformation-et-de-la-communication-tic, consulté en avril 2022

Les fournisseurs de service: Il s'agit des entreprises dont le cœur de métier consiste à faciliter l'accès aux services TIC. L'on retrouve dans cette catégorie les fournisseurs d'accès Internet, les opérateurs de téléphonie, les hébergeurs.

Les fournisseurs de contenus: Cette catégorie regroupe l'ensemble des structures dont le cœur de métier consiste à créer des contenus accessibles sur Internet. Il s'agit notamment des éditeurs de plateformes de réseaux sociaux (Facebook, Twitter, Telegram, etc), les éditeurs de plateforme de streaming (Netflix, etc), etc.

Les organismes de standardisation: Dans l'optique de promouvoir le libre échange des biens et services, des organismes de standardisation ont été créés à l'effet de définir les normes et standards garantissant l'interopérabilité des produits et services TIC. Parmi les organismes majeurs, l'on peut citer l'UIT (Union Internationale des Télécommunications), l'IEEE (Institute of Electrical and Electronic Engineer), l'ISO (International Standardization Organization).

Les régulateurs: Pour garantir un environnement saint et équitable entre les acteurs TIC installés sur leurs territoires respectifs et assurer une concurrence saine tout en promouvant la vision stratégique de leur Etat dans le domaine TIC, les Etats ont mis en place des structures chargées de réguler ces technologies.

B - IMPACT DES TIC SUR L'ÉCONOMIE

Grâce à leur transversalité et à leur capacité à optimiser les rendements, les TIC se sont imposées dans tous les secteurs d'activités traditionnels et en ont même engendré de nouveaux, se hissant, ainsi, parmi les principaux leviers de développement économique. Leur contribution à l'économie est de deux ordres;

Contribution directe: il s'agit de la contribution en termes de richesse et d'emplois des activités inhérentes aux TIC notamment les télécommunications, la production et la commercialisation des équipements et des logiciels;

Contribution indirecte: il s'agit de la contribution induite par le gain de performance des secteurs traditionnels (agriculture, finance, transport, tourisme, industrie, etc.) due à l'adoption des TIC.

Compte tenu de l'ampleur prise par ces technologies, l'Union Internationale des Télécommunications (UIT) a conçu un indice dénommé IDI (ICT

development index) destiné à mesurer l'évolution des TIC au niveau de chaque pays. La figure ci-dessous illustre les résultats d'une étude menée sur la corrélation entre le IDI et le PIB.

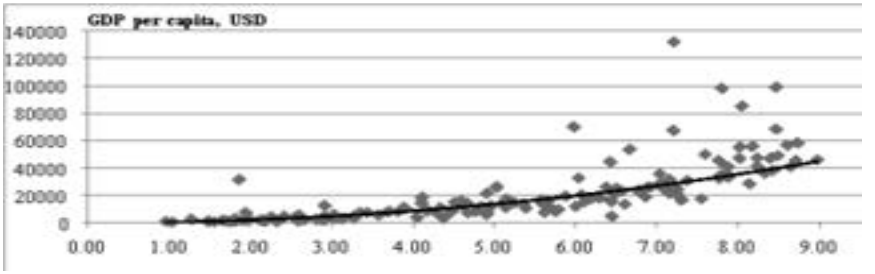


Figure N°1: corrélation entre le PIB par habitant et le niveau de l'IDI en 2017
Source: Y. Bilan, et al., «ICT and economic growth: links and possibilities of engaging», Intellectual Economics, N°13, 2019, p.6.

De ce graphe, il ressort clairement que l'évolution du PIB est positivement corrélé à celui de l'IDI ce qui pourrait laisser penser que plus un pays développe son économie numérique, plus il accélère sa croissance. De même, d'après une étude de la Banque Mondiale, une augmentation du taux de pénétration du broadband mobile de 10% en Afrique entrainerait une augmentation du PIB de 2.5%.

Selon le Rapport Digital Economy Report 2019 de l'ONU, l'économie numérique représentait **11 500 milliards de dollars**[2], soit **15,5 %** du PIB mondial (**18,4 %** du PIB dans les économies développées et **10 %** dans les économies en développement en moyenne). Le rapport mentionne que l'économie numérique avait augmenté deux fois et demie plus vite que le PIB mondial au cours des 15 années précédentes, doublant presque d'envergure depuis 2000. A cause de la fracture numérique, les retombées de cette économie ne sont pas équitablement distribuées sur le globe: les Etats-Unis représentent 35% de cette économie, l'Union Européenne 25%, la Chine 13%, le Japon 8%. Ce constat pourrait être lié au fait que le taux de pénétration des TIC en général et de l'Internet n'est pas uniforme dans tous les pays du monde comme l'atteste la figure ci-contre.

[2] UN-UNCTAD, «DIGITAL ECONOMY REPORT 2019 - Value creation and capture implications for developing countries», New York, United Nations Publications, 2019, p.69.

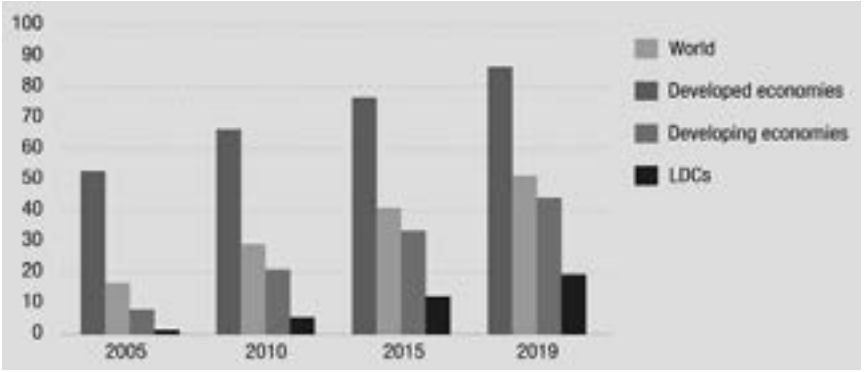


Figure N°2: Evolution du niveau de connectivité en fonction du niveau de développement
Source: UN-UNCTAD, «DIGITAL ECONOMY REPORT 2021 Cross-border data flows and development», New York, United Nations Publications, 2021, p.13

De cette figure, il ressort que le taux de pénétration de l'Internet dans les pays développés est passé d'environ 50% en 2005 à plus de 80% en 2019 alors que dans les pays en voie de développement, il est passé d'environ 5% à près de 40% sur la même période. Ce qui confirme effectivement la fracture numérique qui est un problème central pour le développement.

La figure ci-dessous illustre la répartition des parts de marché des différents segments de marchés (matériel, logiciel, télécommunications, prestations de service et nouvelles technologies) du secteur des TIC à travers le monde entre 2018 et 2021.

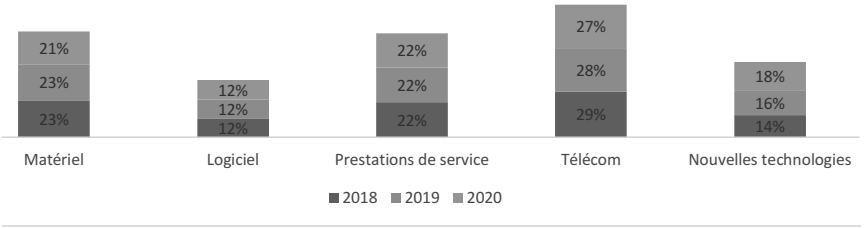


Figure N°3: Répartition des parts de marché des différents segments de marchés du secteur des TIC à travers le monde entre 2018 et 2021.

IDC Corporate USA, «IDC - Global ICT Spending Forecast 2020 – 2023», IDC, 2020, Source:https://www.idc.com/promo/global-ict-spending/forecast, consulté en avril 2022.

Les TIC sont en passe d'apporter un changement profond dans l'univers

de la finance à travers les cryptomonnaies. Le marché de la cryptomonnaie qui était estimé à 81 milliards en 2012 est estimé en 2022 à environ 774 milliards de dollars. De même, le bitcoin valait 7.75$ en 2012 et en 2022 il vaut 407.772$.

Le Cameroun n'est pas resté en marge de cette mouvance vers la modernité impulsée par les TIC car le gouvernement a mobilisé d'importants moyens ces dernières années, malgré la conjoncture difficile, pour développer ce secteur à travers la densification du réseau de fibre optique national qui atteint désormais 20.000Km, la diversification des points d'atterrissement (notre pays compte actuellement cinq points d'atterrissement), le déploiement de deux points d'échanges Internet à Yaoundé et à Douala, la construction de plusieurs incubateurs de startup. Les efforts de l'Etat ont entraîné une augmentation du taux de pénétration de l'Internet, qui est passé de 4.3% en 2010 à plus de 40% en 2022, une réduction des coûts d'accès aux terminaux TIC, et une prolifération des e-services au Cameroun avec l'éclosion de plusieurs startups. Par ailleurs, l'industrie des TIC apparaît comme le deuxième pourvoyeur d'impôts au Cameroun, après les industries pétrolières.

C - IMPACT SOCIO-CULTUREL

Les TIC de par leur gain de popularité observé dans tous les secteurs d'activités notamment l'audiovisuel, la communication et l'industrie du divertissement sont devenus un levier important de domination culturelle. Il apparait donc logique que les USA qui possèdent les principales infrastructures de l'Internet aient réussi à imposer leur culture à travers le monde. Il convient tout de même de relever que la domination américaine remonte à la fin de la deuxième guerre mondiale où les Etats-Unis, grand vainqueur vont proposer à travers le plan Marshall une aide au développement de l'Europe décimée par la guerre: ce qui va permettre aux Etats-Unis d'imposer leur vision du monde.

Aujourd'hui, le «rêve américain» et l'*American way of life* sont des modes de vie les plus populaires et auxquelles aspirent la plupart des jeunes du monde entier.

L'un des vecteurs de la diffusion de la culture américaine est la langue. D'après une étude réalisée par HOOTSUITE[3] l'anglais est la langue la plus populaire sur Internet avec près de 60%. En ce qui concerne l'industrie du divertissement qui occupe une part importante dans la culture, l'on note que les plateformes de musique en streaming les plus populaires sont des plateformes américaines comme l'illustre la figure ci-après:[3]

Figure N°4: Marché de souscription de la music dans le mode

Source: A. Parker, «The Global Music Subscriber Market is Out with Its Status for Q1 2021», Daily MusicRoll Online Music Magazine, 2021, https://www.dailymusicroll.com/entertainment/the-global-music-subscriber-market-is-out-with-its-status-for-q1-2021.html, consulté en avril 2022.

Le constat est le même dans le secteur du streaming vidéo ou de la vidéo à la demande où les plateformes telles que Netflix, HBO, Disney+, Prime caracolent en tête du classement. De même, considérant le rôle important des maisons de production dans cette industrie, nous avons observé d'après le tableau suivant, que les plus importantes maisons de productions de film sont américaines.

[3] **We Are Social & Hootsuite**, « DIGITAL 2022: LANGUAGE, CULTURE, AND GLOBAL CONTENT HABITS», *Data Reportal*, 2022, https://datareportal.com/reports/digital-2022-language-culture-and-content, consulté en avril 2022.

Figure N°5: Part de marché des films par pays
Source: Nash Information Services, LLC, «Movie Production Countries», The Numbers, 2022, https://www.the-numbers.com/movies/production-countries/#tab=territory, consulté en avril 2022.

Internet grâce à sa nature interconnectée et maillée a contribué à renforcer la mondialisation ainsi que le brassage culturel en permettant à des individus et des organisations situés de part et d'autre du globe de communiquer et d'interagir. Cependant, des dérives ou des troubles au comportement social peuvent être observés chez certains individus qui à cause du sentiment de bulle ou d'addiction que peut procurer cette technologie, se déconnectent de leur environnement social.

II - CYBERSÉCURITÉ ET CYBERCRIMINAMITÉ

A - CONTEXTE

Compte tenu de l'engouement suscité par les TIC auprès des populations et de leur implication dans tous les secteurs d'activité, de nouvelles menaces, connues sous le vocable de cybercriminalité, profitant de la virtualité de ce nouvel environnement qu'est le cyberespace et du sentiment d'anonymat qu'il procure pour perpétrer des actes malveillants, ont vu le jour. La cybercriminalité se définit communément comme l'ensemble des infractions commises sur ou au moyen des TIC. La cybersécurité, quant à elle, désigne l'ensemble des moyens organisationnel, physique et technique permettant de garantir la sécurité des actifs

cybernétiques. Elle repose sur quatre (04) principes cardinaux que sont :

La confidentialité: ce principe traduit l'aptitude d'une information à être intelligible uniquement par des entités autorisées;

L'intégrité: il s'agit de l'aptitude d'une information à demeurer intacte, à ne pas être altéré durant la communication.

La disponibilité: ce principe traduit l'aptitude d'une information à demeurer permanemment accessible par les entités autorisées;

La non répudiation: il s'agit d'un principe qui garantit le fait que les actions opérées par des individus sur des actifs des systèmes d'information ne puissent pas être niées par ceux-ci.

B - LES CYBERCRIMES

Avec le gain de popularité et l'évolution qu'ont connus les TIC, l'on a assisté au développement de techniques d'attaques de plus en plus diverses et sophistiquées. D'après le magazine «cybercrime magazine» les pertes dues à la cybercriminalité qui en 2015 étaient estimées à 3000 milliards US$ ont atteint 6000 milliards de dollars en 2021[4] et pourraient s'accroître à 10.000 milliards d'ici 2025. Parmi les techniques d'attaque les plus populaires l'on peut citer :

Le phishing: Il s'agit d'une forme d'attaque consistant pour les cybercriminels à leurrer les victimes via des artifices savamment orchestrées qui exploitent la faille humaine, pour les amener à fournir leurs informations sensibles qui seront ensuite utilisées à des fins malicieuses.

Les fakes news: fort de la popularité des médias sociaux, des individus malintentionnés ont profité de la célérité et de la popularité de ces canaux pour diffuser des fausses informations à des fins diverses notamment la propagande, etc.

Les dénis de service: il s'agit des attaques qui consistent à compromettre la disponibilité des actifs des systèmes d'information

[4] S. Morgan, «Cybercrime Damages $6 Trillion By 2021» *Cybercrime Magazine*, 2017, https://cybersecurityventures.com/annual-cybercrime-report-2017, consulté en avril 2022

notamment en saturant ceux-ci par des requêtes fallacieuses et intempestives**.**

Les ransomware: il s'agit d'une d'attaque consistant à utiliser des codes malveillants pour prendre en otage les données d'un système d'information à travers des mécanismes de cryptographie et exiger de la victime le paiement d'une rançon.

Les trojan: Ce sont des codes malveillants dissimulés dans des logiciels authentiques dans l'optique de perpétrer des actions illicites sur les ordinateurs sur lesquels ces logiciels sont installés.

Les virus: est un terme générique qui désigne l'ensemble des logiciels destinés à effectuer des actes malveillants dans un système d'information notamment en portant atteinte à la confidentialité, l'intégrité et la disponibilité des actifs informationnels.

Les botnet: C'est un réseau d'ordinateurs infectés qui peuvent être contrôlés à distance pour envoyer du spam, répandre des malwares ou lancer des attaques de déni de service, le tout sans le consentement du propriétaire de ces appareils[5].

Les **APT (advanced persistent threat)**: Il s'agit d'une intrusion informatique ciblée dans laquelle l'attaquant recherche une présence à long terme sur le système compromis, en demeurant furtif. Ce type d'attaques a connu une nette recrudescence ces dernières années car il serait, de plus en plus, utilisé par des Etats ou des Organismes à des fins d'espionnage ou de sabotage[6].

Avec le développement des techniques de chiffrement de plus en plus sophistiquées, un espace reconnu comme étant le lieu par excellence d'hébergement des contenus malveillants et connu sous le vocable de **DARK WEB** s'est développé. D'après la société Kaspersky spécialisée sur les questions de cybersécurité[7], cet espace regorge plus de 90% du contenu de l'Internet. Il a la particularité d'être anonyme en ce sens que des mécanismes

[5] Avast, « Qu'est-ce qu'un botnet ?», *Avast*, 2022, https://www.avast.com/fr-fr/c-botnet, consulté en avril 2022.
[6] F. Puybareau, « Advanced Persistent Threat (APT)», *Les Assises*, https://www.lesassisesdelacybersecurite.com/Le-blog/Glossaire/Advanced-Persistent-Threat-APT, consulté en avril 2022.
[7] AO Kaspersky Lab, « Que sont le Deep Web et le Dark Web ?», *Kaspersky*, https://www.kaspersky.fr/resource-center/threats/deep-web, consulté en avril 2022.

spéciaux y ont été déployés pour rendre les identités anonymes et les communications inintelligibles même pour les services de sécurité. Pour y accéder, il faut utiliser des navigateurs spéciaux tels que ***Tor*** et des moteurs de recherche dédiés. Il héberge des contenus tels que les sites web de vente de drogue, d'armes, les sites web de recrutement des tueurs à gage, les sites web d'achat de virus ou de logiciel malveillant et même des sites web permettant de louer des services d'un hacker professionnel pour une tâche précise.

C - LUTTE CONTRE LA CYBERCRIMINALITÉ

Pour faire face à la cybercriminalité, les Etats ont dû revoir leur organisation pour créer des structures dédiées. Dans les pays développés qui ont pris conscience de l'importance de la menace cybernétique, il a été créé une structure civile chargé de la cybersécurité et une autre militaire chargée de la cyberdéfense. C'est le cas aux Etats-Unis avec le DHS (Department of Homeland Security) qui a la charge de la sécurité des infrastructures cybernétiques civiles et le US CYBERCOM qui travaille étroitement avec la NSA (National Security Agency) et qui en plus d'assurer la sécurité des infrastructures cybernétiques militaires et des infrastructures critiques civiles a aussi des missions offensives. Pour la plupart des pays en voie de développement, le volet cyberdéfense n'est pas encore pris en compte, les cyber-menaces sont confiées à la charge d'une structure civile qui ne gère que la cybersécurité et donc n'aborde pas encore les cybermenaces d'un point de vue stratégique.

Pour gérer la cybersécurité à l'échelle nationale, les Etats ont recours à une stratégie qui s'appuie sur quatre (04) grands axes :

La dissuasion: Cet axe définit l'ensemble des actions entreprises par un Etat pour dissuader toute attaque informatique sur une de ses infrastructures. Pour des cas de cybercriminalité classiques, les dispositions de sanctions prévues dans le cadre légal rentrent dans ce registre. Pour des attaques stratégiques, certaines puissances, notamment, les Etats-Unis envisagent à travers le *cyber deterrence policy* élaboré en 2015 sous l'administration Obama, une riposte militaire en cas de cyberattaque avérée sur leurs installations stratégiques.

La prévention: Cet axe regroupe l'ensemble des dispositions d'ordre

organisationnel et technique destinées à mitiger ou annihiler les risques d'attaques cybernétiques.

La détection: Cet axe porte sur les mesures à prendre pour détecter le plus rapidement possible les tentatives d'attaques ou d'intrusion dans les infrastructures critiques.

La réaction: Il s'agit des actions visant à assurer une réponse rapide et efficace aux attaques qui auront réussi à traverser le bouclier défensif.

Sur un plan opérationnel, les actions des Etats s'articulent généralement autour des activités suivantes;

La sensibilisation: Ayant pris conscience de l'implication massive des failles humaines dans la plupart des attaques d'envergure, il est apparu indispensable pour les Etats de dédier des programmes entiers pour la sensibilisation des populations sur la cybersécurité;

La formation: Vu l'importance sans cesse grandissant des TIC et des cybermenaces dans la société, il est plus que jamais nécessaire, pour les Etats, de disposer des ressources humaines qualifiées et en quantité suffisante dans les domaines de la cybersécurité et de la cyberdéfense. C'est ce qui justifie l'accroissement ces dernières années, du nombre de programme de formations et de recherche et développement dans ces domaines;

L'élaboration des normes et référentiels: Afin de prémunir les systèmes d'informations d'attaques informatiques, des normes et standards ont été développés dans le monde notamment ISO 27001, PCI-DSS, NIST SP-800, etc. Des Etats, soucieux de la sécurité de leur cyberespace, se sont appropriés ces normes et pour certains les ont transcrites fort du contexte local, puis ont mis en place des mécanismes légaux pour amener voire obliger les structures installées sur leur territoire à mettre en application lesdits référentiels;

Le déploiement des plateformes de cybersécurité: Pour assurer la sécurité de leur cyberespace, les Etats sont amenés à déployer dans des emplacements spécifiques, des dispositifs spéciaux de cyberdéfense notamment les firewalls, des systèmes de protection contre les intrusions, les dispositifs d'interception des communications, etc.

Les cyberdrill: Il s'agit d'exercices de simulation d'attaques en

grandeur nature, destinés à éprouver les systèmes de défense cybernétique des nations. Les pays développés ont recours à ce type d'exercice au moins une fois l'an.

III - LE CYBERESPACE COMME INSTRUMENT DE PUISSANCE

De tout temps, l'histoire du monde a été marquée par la naissance et le déclin de certains empires qui chacun à leur tour, à leur époque ont usé des leviers de l'heure pour asseoir leur domination sur le monde. Les TIC de par leur nature première d'outil de traitement et de stockage de l'information qui, convient-il de le rappeler est la matière première du 21eme siècle s'impose comme un levier important de puissance pour les Etats qui peut redessiner une nouvelle carte géopolitique du monde.

Dans les relations internationales, la puissance désigne la capacité d'un acteur à obtenir des autres acteurs qu'ils infléchissent leurs actions et leurs conduites dans le sens de ses propres intérêts, sans consentir en retour de concessions de même valeur.

Joseph Nye, chercheur de renommé dans les relations internationales a théorisé la puissance sous deux (02) angles: le hard power et le soft power.

Dans son livre *Bound to Lead - The Changing Nature of American Power*[8], après avoir défini ces deux composantes, il a recommandé l'usage combiné et mesuré de ces deux facteurs pour une meilleure efficacité à travers un nouveau concept dénommé smart-power. Les sections suivantes seront consacrées à l'impact potentiel du cyberespace dans ces deux (02) dimensions de la puissance.

A - LE CYBERESPACE COMME INSTRUMENT DE HARD POWER

Le *hard-power* désigne la faculté d'une partie d'imposer une ligne de

[8] J. S.Nye, *Bound to Lead - The Changing Nature of American Power*, New York, Basic Books, 1990-1991, pp.25-49.

conduite à d'autres par la coercition. Dans le monde physique, cette coercition peut être exercée par les armes ou la suprématie technologique et économique.

Comme présenté dans la première partie de cet article, les technologies de l'information et de la communication occupent une place centrale dans les différents secteurs d'activités notamment la finance, la santé, l'agriculture, l'énergie, le transport, etc. Les plateformes boursières, les centrales énergétiques, les systèmes de gestion de transport sont entièrement contrôlés par des outils informatiques.

Ainsi, une attaque ciblée sur une infrastructure critique d'un Etat (système de contrôle des trains, système de contrôle des feux de signalisation, système de gestion des banques, etc) peut paralyser celui-ci et le faire retourner à l'âge de pierre.

A titre d'illustration, nous pouvons citer :

L'attaque stuxnet qui rentre dans la catégorie des APT (*Advanced Persistent Threat*) définie dans la section précédente, aurait été orchestrée par Israël et les Etats-Unis pour ralentir le programme d'enrichissement nucléaire iranien. A travers des techniques de pointe, ces gouvernements auraient infiltré des codes malveillants difficiles à détecter dans les systèmes SCADA (systèmes informatiques permettant de gérer des dispositifs industriels) qui pilotaient les centrifugeuses de la centrale de *Natanz*. Cette attaque qui a été détectée en 2010, aurait retardé le programme nucléaire iranien de deux (02) ans;

L'attaque estonienne: Le 27 avril 2007, la quasi-totalité des principaux systèmes informatiques gouvernementaux et bancaires estoniens ont été paralysés pendant plusieurs heures à cause d'une attaque informatique de type déni de service distribué (DDos). D'après les investigations, cette attaque d'envergure provenait de Russie et aurait été intenté par le gouvernement Russe en signe de représailles ou de protestation au déplacement par les autorités estoniennes de la statue de bronze, monument érigé en l'honneur de l'Armée Rouge, du centre de la capitale à Tallinn vers la banlieue. La Russie ayant interprété cet acte comme le rapprochement

de l'Estonie du bloc occidental, aurait décidé de lancer cette attaque.

L'impact des TIC sur le *hard-power* est d'autant plus important que de nos jours toutes les armes lourdes modernes sont basées sur ces technologies. L'on peut citer les systèmes de guidages de missiles, les drones militaires, les radars, les systèmes de contre-mesure, etc. La maîtrise des TIC par un belligérant pourrait donc lui conférer un avantage tactique voire stratégique sur les théâtres d'opération.

B - LE CYBERESPACE COMME INSTRUMENT DE SOFT POWER

Le soft power se définit par la capacité d'un État à influencer et à orienter les relations internationales en sa faveur par un ensemble de moyens autres que coercitifs (menace ou emploi de la force) notamment par l'attraction et la persuasion. Du fait que les TIC sont l'outil par excellence pour traiter, conserver et transmettre les informations, elles ont un impact important sur l'influence des tendances d'opinions.

En effet, le développement des offres 3G/4G/5G qui permettent d'avoir accès à Internet à large bande sur un téléphone portable combiné à la recrudescence de l'usage des plateformes de réseaux sociaux a instauré un nouveau paradigme dans le domaine de la communication: Toute personne muni d'un smartphone et d'une connexion internet peut désormais être une source d'une information qui se répand à la vitesse de la lumière et atteint les différentes parties du globe en quelques minutes. Le pouvoir de diffuser l'information qui autrefois était réservé à une poignée d'organismes, à qui une régulation stricte était appliquée avec des normes relatives à la vérification des informations avant diffusion, est désormais conféré au commun des internautes sans aucune procédure: ce qui a pour corollaire la prolifération des *fakes news*.

Le taux de pénétration des réseaux sociaux est de 58.4% dans le monde[9], 20.7% en Afrique[10] et 16.5% au Cameroun[11]. Grace à leur popularité et la

[9] We Are Social & Hootsuite, «*DIGITAL 2022: GLOBAL OVERVIEW REPORT*», Data Reportal, 2022, https://datareportal.com/reports/digital-2022-global-overview-report, consulté en avril 2022.
[10] D. Kodjani, « Utilisation D'Internet En Afrique De L'Ouest En 2021», Afro Aware, 2021, https://afroaware.com/2021-

vitesse avec laquelle ils acheminent l'information, le web et les réseaux sociaux en particulier se sont hissés aux premières loges des canaux de communication. D'après une étude réalisée[12] par la *Société d'investissement et de renseignement dans les médias Magna*, le digital représente aujourd'hui 62% des dépenses en marketing et ce pourcentage est appelé à augmenter.

C'est conscient du pouvoir des réseaux sociaux qu'aujourd'hui les gouvernements étrangers et même certains organismes privés et individus ont recours aux services des usines à troll pour véhiculer leur idéologie, discréditer une entité, manipuler les opinions et inciter à la haine et à la révolte. Les mouvements sociaux sont désormais initiés et entretenus à travers les plateformes de réseaux sociaux. Le printemps arabe qui a entrainé des révolutions dans la plupart des pays du Maghreb en est une illustration. De même, les multiples soupçons de l'ingérence du gouvernement russe dans les élections présidentielles aux Etats-Unis et même en France au travers de campagne de propagande sur les réseaux sociaux savamment orchestrées en sont une illustration du *soft power* des réseaux sociaux. Il est établi que la culture américaine notamment le «*american way of life*» et le «*american dream*» est la culture la plus populaire à travers le monde. Internet y a contribué pour beaucoup, notamment grâce à la diffusion de musique et de films américains sur les plateformes de streaming[13].

L'accroissement du taux de pénétration de l'Internet combiné à la transformation digitale tout azimut a engendré une explosion du volume de données générées. L'exploitation de ces données constitue un enjeu majeur tant sur le plan économique avec notamment des campagnes marketing ciblées que sur les plans sécuritaire et stratégique avec la collecte et l'analyse des renseignements permettant d'anticiper sur d'éventuelles menaces. C'est conscient de cela que les Etats ont mis en place des

internet-usage-in-west-africa, consulté en avril 2022.

[11] We Are Social & Hootsuite, « *DIGITAL 2022: CAMEROON* «, Data Reportal, 2022, https://datareportal.com/reports/digital-2022-cameroon, consulté en avril 2022.

[12] Magna, «*GLOBAL ADVERTISING MARKET REACHES NEW HEIGHTS, AND EXCEEDS PRE-COVID LEVELS*», Magna, 2021, https://magnaglobal.com/global-advertising-market-reaches-new-heights-and-exceeds-pre-covid-levels, consulté en avril 2022.

[13] J. S.Nye, «*Soft Power 2.0 The Future of Power in the Digital Age* «, *The Dubai Policy Review*.

mécanismes juridiques et techniques permettant de réglementer la collecte, le traitement et le transfert de données vers des pays étrangers. Le RGPD élaboré par l'Union Européenne en est une illustration.

Le *soft-power* des TIC peut aussi se manifester au niveau de l'élaboration des normes et standards et l'innovation. L'élaboration des normes et standards a un impact sur les produits qui sont autorisés à être commercialisés. Ainsi, plus un Etat ou une communauté est impliqué dans le processus d'élaboration des normes et standards, plus cet Etat pourrait orienter les normes vers les spécifications techniques des prototypes développés ou en cours de développement par ses entreprises ou ses laboratoires de recherche ce qui permettra à ces derniers d'avoir un avantage compétitif sur les autres acteurs du secteur. De la même manière, l'innovation donne une avance à la société et à son pays d'origine sur un segment de marché ce qui a une importance sur le plan économique et participe à la promotion de la culture de ce pays. En ce qui concerne l'innovation, compte tenu du fort potentiel des technologies émergentes telles que l'Intelligence artificielle, le *data mining*, l'internet des objets, les nanotechnologies et la *blockchain*, les progrès dans ces domaines vont conférer aux Etats avancés, un avantage stratégique certain.

CONCLUSION

Les TIC représentent un potentiel certain que les Etats se doivent de capitaliser tant pour développer leur économie que pour maîtriser leur contexte socio-culturel. Cependant leur nature virtuelle et maillée a fait naître de nouvelles menaces connues sous le vocable de cybercriminalité. Compte tenu de leur large adoption dans tous les secteurs d'activité notamment les secteurs critiques tels que la défense, la finance, l'industrie, l'énergie et l'éducation et de leur faculté à traiter et transmettre les informations en temps réel, ces technologies se sont imposées comme des leviers importants de puissance (*hard et soft power*) qui animent le jeu des relations internationales et peuvent modifier la configuration géopolitique du globe. Il apparait donc nécessaire pour les Etats de modifier leur cadre

organique et institutionnel et développer des stratégies adéquates pour maitriser ces technologies. Parmi les axes que ces stratégies devront aborder figurent la mise en place d'institutions civiles et militaires dédiées respectivement à la cybersécurité et à la cyberdéfense, la mise en place d'un cadre légal régissant les problématiques de cybersécurité, la sensibilisation et la formation, la protection des données personnelles, la sécurité des infrastructures critiques, la souveraineté numérique, la recherche et l'innovation et la maitrise des informations diffusées. Aussi, dans un monde multi polaire dans lequel la mondialisation s'impose et les menaces asymétriques sont de plus en plus populaires, il serait indiqué de trouver le juste milieu entre la préservation de la souveraineté et l'intégration dans le village planétaire.

BIBIOGRAPHIE

1 **Avast**,»Qu'est-ce qu'un botnet?»,https://www.avast.com/fr-fr/c-botnet,consulté 2022.

2 **CoinGecko**,»Cryptocurrency Global Charts», CoinGecko, 2022, https://www.coingecko.com/en/global_charts, consulté en avril 2022.

3 **D. Kodjani**, « Utilisation d'internet en Afrique de L'Ouest en 2021», Afro Aware, 2021, https://afroaware.com/2021-internet-usage-in-west-africa, consulté en avril 2022.

4 **ESCP BUSINESS SCHOOL**, «DIGITAL RISER REPORT 2021», Berlin, 2021.

5 **F. Puybareau**, «Advanced Persistent Threat (APT)», Les Assises, https://www.lesassises delacybersecurite.com/Le-blog/Glossaire/Advanced-Persistent-Threat APT, consulté en avril 2022.

6 **IDC Corporate USA**, «IDC - Global ICT Spending Forecast 2020 – 2023», IDC, 2020 https://www.idc.com/promo/global-ict-spending/forecast, consulté en avril 2022.

7 **J. S.Nye**, «Soft Power 2.0 the Future of Power in the Digital Age «, the Dubai Policy Review.

8 **J. S.Nye, Bound to Lead** - The Changing Nature of American Power, New York, Basic Books, 1990-1991.

9 **J. S.Nye, Soft Power**: The Means to Success in World Politics, New York, Public Affairs, 2004.

10 **Kaspersky AO Lab**, « Que sont le Deep Web et le Dark Web ?», Kaspersky, https://www.kaspersky.fr/resource-center/threats/deep-web, consulté en avril 2022.

11 **Magna**, «GLOBAL ADVERTISING MARKET REACHES NEW HEIGHTS, AND EXCEEDS PRE-COVID LEVELS», Magna, 2021, https://magnaglobal.com/global-advertising-market-reaches-new-heights-and-exceeds-pre-covid-levels, consulté en avril 2022.

12 **Nash Information Services LLC**,»Movie Production Countries», The Numbers, 2022,

https://www.the-numbers.com/movies/production-countries/#tab=territory,consulté,avril2022.

13 **Parker A.**, «The Global Music Subscriber Market is Out with Its Status for Q1 2021», Daily MusicRoll Online Music Magazine, 2021, https://www.dailymusicroll.com/entertainment/the-global-music-subscriber-market-is-out-with-its-status-for-q1-2021.html, consulté en avril 2022.

14 **S. Morgan**, «Cybercrime Damages $6 Trillion By 2021» Cybercrime Magazine, 2017, https://cybersecurityventures.com/annual-cybercrime-report-2017, consulté en avril 2022

15 **UNESCO-Institut statistique**, «Glossaire FR», Technologies de l'information et de la communication (TIC), http://uis.unesco.org/fr/glossary-term/technologies-de-linformation-et-de-la-communication-tic, consulté en avril 2022.

16 **UN-UNCTAD**, «DIGITAL ECONOMY REPORT 2021 Cross-border data flows and development», New York, United Nations Publications, 2021.

17 **We Are Social & Hootsuite**, «DIGITAL 2022: GLOBAL OVERVIEW REPORT», Data Reportal, 2022, https://datareportal.com/reports/digital-2022-global-overview-report, consulté en avril 2022.

18 **Y. Bilan et al**., «ICT and economic growth: links and possibilities of engaging», Intellectual Economics, N°13, 2019.

DEPLOIEMENT DES NOUVEAUX MAITRES D'INTERNET: TYPOLOGIE, RATIONALITE ET MODES OPERATOIRES DES ACTEURS DOMINANTS DU CYBERESPACE

BABA WAME[1]
Docteur en Journalisme et enseignant à l'ESSTIC, spécialiste des TIC

RESUME

En moins d'un quart de siècle, les GAFAM se sont imposés à la tête de l'industrie numérique mondiale. L'acronyme doit son nom aux initiales des entreprises Google, Amazon, Facebook, Apple et Microsoft. Ces cinq géants atteignent, à eux seuls, **une capitalisation boursière de 4,5 billions de dollars.** Ils font tous partie des dix entreprises américaines les plus cotées. Elles sont toutes listées au Nasdaq. Elles sont rejointes, depuis quelques années, par les NATU, quatre grandes sociétés américaines innovantes, symboles de l'économie désintermédiée et par les BATX chinoises qui ne voudraient pas se laisser distancer par les Américains dans la conquête du monde numérique.

Ces superpuissances économiques s'imposent en véritables maîtres dans leur domaine. Ainsi, Google est utilisé dans plus de 90 % des recherches sur Internet. Après avoir racheté YouTube pour seulement 1,65 milliard de dollars en 2006, l'entreprise voit son diffuseur de vidéo en ligne concentrer un nombre de vues bien plus élevé que toutes les chaînes de télévision. De

[1] E-mail: babawame@gmail.com, Phone: +237 696 96 98 96

son côté, Facebook enregistre tous les mois des chiffres supérieurs à 2,7 milliards d'utilisateurs. Dans le secteur des smartphones, c'est Apple qui cumule 32 % du chiffre d'affaires du marché et 66 % des bénéfices qui en découlent. Amazon frôle le monopole et continue de ringardiser des millions de commerces. Enfin, Microsoft est omniprésent sur le marché informatique avec un système d'exploitation présent dans 90 % des ordinateurs au monde.

Au fil des années, ces acteurs dominants du cyberespace ont créé de véritables monopoles qui leur permettent de réaliser des chiffres d'affaires colossaux. Ils utilisent notamment ces moyens pour neutraliser, en la phagocytant, toute éventuelle concurrence. Pour se faire une idée de leurs modes opératoires, il faut comprendre leurs aspirations profondes mêlées d'une volonté de dépasser les limites de l'humain, de proposer une nouvelle politique mondiale et d'imposer des monopoles sectoriels avec, pour ambition sous-jacente, la mainmise sur les données des internautes, des entreprises et des Etats.

INTRODUCTION

Tout aurait débuté dans les années 1960 et probablement bien avant avec Arpa[2] puis ArpaNet[3] dans des laboratoires de l'armée américaine. Un système de communication indestructible et tentaculaire, maillant la planète entière en est sorti. Cette toile numérique encore appelée cyberespace, démesurément agrandie par la téléphonie mobile, a profondément modifié notre rapport aux autres. Univers en construction, le cyberespace demeure encore un espace ouvert où les acteurs les plus divers se côtoient et s'affrontent quelquefois sans que personne n'ait encore imposé sa règle du jeu. Son universalité en fait, encore en 2022, un *no man's land* où les lignes de force sont mouvantes. Internet ressemble à s'y méprendre à ces grands espaces «supposés» vierges du 18ème siècle que les nations occidentales se disputaient. Navigateurs, marchands, militaires et évangélistes s'y

[2] Advanced Research Projects Agency
[3] Advanced Research Projects Agency Network

bousculaient. Chacun prétendant porter la vision éthérée de l'avenir pour le nouveau monde. Pour beaucoup, le réseau des réseaux est un nouvel Eldorado, pour d'autres, une terre de liberté et enfin pour les plus mercantiles, c'est une contrée sauvage à civiliser. Internet ne souffre pas d'une absence de pouvoir et de droit, mais bien plutôt d'un trop-plein, d'une surabondance de petits seigneurs avides de s'étendre à partir de leur domaine respectif et de saisir les opportunités du Nouveau Monde.

Au fil des ans, le système d'échange et de partage de l'information développé par Robert Elliot Kahn[4] et Vinton Cerf, à l'orée des années 1970, s'est transformé en une grande foire où se déchaînent les appétits les mieux aiguisés mais aussi les plus insidieuses. C'est cette arène de temps modernes qui donna naissance aux géants de la technologie et du numérique, acteurs dominants du monde grâce au Big Data. Ils sont majoritairement américains (les GAFAM[5] et les NATU[6]) mais également chinois (Les BATX[7]). De petites start-up au début de ce siècle, ils sont devenus des empires économiques hyper puissants dont certains seraient plus puissants que les Etats. Ils sont les nouveaux maîtres du monde.

Evoquer la puissance nouvelle que représentent ces nouveaux maîtres d'Internet n'est guère aisé, à moins de l'aborder en des termes heuristiques, à défaut, on se vautrerait dans le sensationnalisme et la réification, tant ils fascinent, émerveillent, inquiètent, et font trembler les plus grandes nations dominantes du monde. Pour ces dernières, les GAFAM, NATU et autres BATX sont des OVNI[8] parce qu'inclassables et surtout parce que notre appréhension ainsi que notre perception du monde sont de plus en plus tributaires d'outils que proposent ces entreprises.

Considérer les GAFAM, NATU et BATX comme les nouveaux maîtres du monde revient à battre en brèche la notion d'Etat selon Montesquieu (1748) dans *De l'esprit des lois*. Dès lors, la tentation de céder à des conglomérats économiques, fussent-ils les plus puissants, les plus

[4] Co-auteur avec Vinton Cerf de la base technologique d'Internet, le protocole TCP/IP et inventeur du mot Internet
[5] GAFAM, acronyme de Google, Apple, Facebook, Amazon et Microsoft
[6] NATU, acronyme des entreprises américaines: Netflix, Airbnb, Tesla et Uber
[7] BATX, acronyme des entreprises chinoises du numérique: Baidu, Alibaba, Tencent et Xiaomi
[8] Objet volant non identifié

dominants, les plus grands et les plus prestigieux dans leur secteur spécifique, sanctionnerait une série de transformations fondamentales du lexique politique et international, avec pour risque de les assimiler à une sorte de révolution copernicienne de la géopolitique. Ce nouveau système qui fonde son essence sur le numérique dissoudrait celui de l'Etat westphalien. Les Etats ne seraient donc plus que des constellations orbitales, des boute-en-train d'un spectacle dont les grandes entreprises du Nasdaq[9] joueraient les premiers rôles.

I - LES ACTEURS DOMINANTS DU CYBERESPACE

Les géants de la technologie et du numérique gagnent jour après jour en influence.

A l'heure du Web et de l'information en mobilité, les téléphones portables et les réseaux sociaux sont omniprésents dans nos vies faisant des mastodontes du digital des incontournables. Assis sur des Himalaya des données, de nos données que nous cédons très souvent gratuitement, ces titans du numérique construisent graduellement ce dont ont toujours rêvé les plus grands hommes politiques: un empire mondial dont le maillage s'étendrait jusqu'aux contrées les plus reculées de la planète. Quelles sont ces entreprises qui sont devenus plus puissantes que les Etats, leurs modes opératoires, que font-elles de nos données ? Découvrons ces acteurs dominants du cyberespace qui sont en train de dessiner les contours d'un nouvel impérialisme.

A - LES GAFAM

L'acronyme GAFAM désigne les cinq entreprises américaines du secteur de la technologie et du numérique les plus populaires et cotées en bourse: Google, Apple, Facebook, Amazon et Microsoft. Elles sont également surnommées *The Big Five*. Ces cinq géants se sont imposés

[9] Bourse où sont cotées les entreprises du numérique.

comme des acteurs économiques et politiques majeurs. La capitalisation des GAFAM est au premier trimestre 2022 de plus de 1 000 milliards de dollars pour chacune d'entre elles. Un chiffre colossal qui équivaut au PIB du 17e pays le plus riche du monde. Ils font tous partie des dix entreprises américaines les plus cotées. La plus ancienne de ces cinq entreprises est **Apple, dont l'introduction en bourse date de 1980.** Viennent ensuite Microsoft en 1986, Amazon en 1997, Google en 2004 et Facebook en 2012.

1 - MICROSOFT

Multinationale informatique américaine fondée en 1975 par Bill Gates et Paul Allen, Microsoft fait partie des premières entreprises numériques à avoir révolutionné notre quotidien. Elle s'est faite connaître en développant des systèmes d'exploitation et des logiciels, les plus connus étant le système d'exploitation Windows et la suite bureautique Office (incluant Word, Excel et Power Point). L'entreprise de Redmond équipe aujourd'hui près de 90 % des ordinateurs de la planète.

2 - APPLE

Créée le 1er avril 1976 à Los Altos en Californie, Apple s'est distinguée par la commercialisation d'ordinateurs en lançant dans les années 1980 la gamme des Macintosh, rejoints en 2001 par la gamme des baladeurs numériques «iPod». Mais c'est en 2007, avec la sortie de son produit emblématique l'iPhone, qu'Apple bouleverse le marché de la téléphonie mobile. L'ergonomie révolutionnaire et le magasin d'application «App Store» changeront à tout jamais nos habitudes de vie. Au premier trimestre 2022, Apple concentrait, à elle seule, 32 % du chiffre d'affaires, 66 % des bénéfices du marché des smartphones avec une capitalisation de 2913 milliards de dollars et un résultat net de 94,680 milliards de dollars.

3 - AMAZON

Jeff Bezos fonde en juillet 1994 Amazon. Son modèle économique, le commerce en ligne avec une spécialisation dans la vente de livres, puis il

ouvre sa Marketplace à d'autres types de produits et de revendeurs. Outre sa plateforme, l'avantage compétitif d'Amazon vient de sa chaîne logistique, s'appuyant sur plusieurs types de terminaux (entrepôts de stockage, distribution, points relais) et sur un réseau mondial. Depuis deux ans, Amazon propose aussi des services grand public comme le service de streaming Amazon Prime Vidéo**.** Aujourd'hui, l'entreprise emploie plus d'1 million de salariés dans le monde.

4 - GOOGLE

C'est le 4 septembre 1998 à Menlo Park que Google voit le jour. Moteur de recherche, il est devenu (et reste) dominant dans ce secteur. L'entreprise fondée par Sergueï Brin et Larry Page concentre à elle seule plus de 90 % des requêtes mondiales sur Internet. En 2006, l'entreprise a racheté YouTube qui compte bien plus de vues que n'importe quelle chaîne de télévision (1 milliard d'heures de vidéo sont regardées chaque jour). En 2015, Google est devenue une filiale de la nouvelle maison-mère Alphabet, conglomérat de nombreuses sociétés technologiques.

5 - FACEBOOK

Facebook, que l'on peut traduire en français par trombinoscope, est un réseau social créé en février 2004 appartenant à la société Meta. Il est le premier réseau social généraliste permettant à ses utilisateurs à la fois d'envoyer des messages et d'échanger ou publier différents contenus (documents, vidéos, photos, etc.), entre autres fonctions. Le nombre total d'utilisateurs actifs de Facebook en janvier 2022 dépassait les 2,91 milliards dont 4 millions d'utilisateurs au Cameroun. L'entreprise a fait l'acquisition d'Instagram (2012) et de WhatsApp (2014) confortant ainsi sa position de numéro 1 des réseaux sociaux.

B - LES NATU

Apparu en 2015, l'acronyme NATU désigne quatre sociétés américaines innovantes: Netflix, Airbnb, Tesla et Uber. Elles sont emblématiques de

l'économie désintermédiée et pèsent des milliards de dollars en Bourse. Cet acronyme est consubstantiel à un autre acronyme: GAFAM. Si les GAFAM se distinguent par leur réussite sur le marché du numérique, les NATU, elles, ont bâti leur succès sur un **nouveau modèle économique** aux antipodes des *business model* traditionnels. En effet, leur stratégie ne repose pas sur la concurrence au sens strict. Elles ne cherchent pas à capter la clientèle d'un concurrent en adoptant la même politique de vente sur un même produit: elles proposent un produit ou un service totalement nouveau.

1 - NETFLIX

Fondée par Reed Hastings et Marc Randolph en 1997, Netflix est une société qui, à l'origine, était spécialisée dans la location de DVD par abonnement. Ses abonnés avaient la possibilité de louer et de recevoir chez eux les films qu'ils souhaitaient. Ils devaient ensuite renvoyer le DVD à Netflix. En 2007, la société est passée en streaming. L'entreprise met à la disposition de ses clients des films et des séries sur une plateforme numérique. Ils y ont accès de n'importe où, n'importe quand, et de manière illimitée, sous réserve qu'ils aient une connexion internet. Au 31 décembre 2021, Netflix comptait 221,84 millions d'abonnés payants dans 190 pays. L'entreprise de Scotts Valley a changé la façon dont nous consommons le divertissement en proposant du contenu en mode ATAWAD (Any Time, Any way, Any Devices) et instantanément.

2 - TESLA

Tesla est une société spécialisée dans les véhicules électriques. Martin Eberhard et Marc Tarpenning, les deux fondateurs s'étaient donnés pour mission de proposer aux automobilistes une voiture écologique qui fonctionnerait grâce à des énergies renouvelables et ce, sans plus de contraintes pour le conducteur. En 2020, Tesla est devenue le constructeur automobile le plus coté de l'histoire avec une capitalisation de plus de 200 milliards de dollars. Elle est le leader mondial du véhicule électrique avec près d'un million de véhicules vendus en 2021. Tesla s'est positionné sur les véhicules 100 % électriques haut de gamme de type berline de luxe et voiture de sport.

3 - AIRBNB

Airbnb est une entreprise qui évolue dans le secteur de la location touristique. Elle met en relation des particuliers disposant d'un logement avec des voyageurs. Nativement, les particuliers pouvaient seulement louer des chambres. Depuis 2009, il est possible d'avoir un appartement ou toute une maison à sa disposition. L'entreprise propose plus de 7 millions de logements sur sa plateforme de réservations en ligne. Elle compte 150 millions d'utilisateurs dans le monde. Plus de 100 000 villes mettent à la disposition des voyageurs et autres touristes des logements Airbnb dans près de 220 pays. Le chiffre d'affaires d'Airbnb a été multiplié par cinq entre 2016 et 2020, passant de 919 millions de dollars à 4,8 milliards de dollars.

4 - UBER

Uber, anciennement UberCab, est basée à San-Francisco en Californie. Fondée en 2007, Uber est une plateforme qui met en relation des clients et des chauffeurs particuliers par le biais d'une application. Il est désormais possible de contacter un chauffeur pour réaliser une course, n'importe quand et n'importe où. Uber s'est imposé dans le transport des passagers et compte 91 millions d'utilisateurs dans le monde. Depuis quelques années, l'entreprise fait évoluer son concept et lorgne plus que jamais vers d'autres marchés. Ainsi, elle développe des services de livraison à domicile, notamment avec «Uber Eats», un service de livraison de repas à domicile ou sur les lieux de travail. L'entreprise ne cesse d'étendre son envergure. Elle a ainsi lancé, «Uber Freight», une plateforme qui facilite la connexion entre les professionnels du transport routier et les expéditeurs.

C - LES BATX

Depuis quelques années, la Chine, animée par l'objectif d'une indépendance renforcée, a vu naître l'équivalent des GAFAM pour porter le déploiement de sa stratégie numérique. Sous l'acronyme BATX nous retrouvons le moteur de recherche Baidu, le site de e-commerce Alibaba, le site de services (messageries, réseau social…) Tencent et l'entreprise

technologique Xiaomi. Malgré leur concentration sur le marché chinois, toutes ces entreprises ont commencé leur expansion dans le reste du monde, notamment aux Etats-Unis et en Europe.

1 - ALIBABA

Alibaba Group, fondée en 1999, a démarré comme *marketplace* (plateforme qui met en relation des acheteurs et des vendeurs sur Internet) B2B[10] avant de se diversifier sur d'autres créneaux. L'entreprise fonctionne comme une «collection» de plateformes de *marketplace* sans jouer le rôle de distributeur direct. On retrouve par exemple «AliExpress», site de commerce en ligne pour la clientèle internationale. Malgré une croissance fulgurante, le géant chinois reste en deçà de son correspondant américain Amazon en termes de chiffre d'affaires (72 milliards de dollars en 2020 vs 296 milliards), de capitalisation boursière (646 milliards de dollars début 2021 vs 1 575 milliards) et de nombre d'utilisateurs. (1 milliard d'utilisateurs actifs annuels vs 2 milliards)

2 - TENCENT

Tencent, créée en 1998, opère dans le secteur des services numériques mobiles. Elle doit sa renommée à son application QQ Instant Messenger, qui a été l'une des premières applications de messagerie instantanée lancée en Chine. WeChat, lancée en 2011, est devenue l'application la plus utilisée en Chine avec plus d'1,2 milliard d'utilisateurs en 2020. En quelques années, Tencent est devenue l'une des entreprises les plus rentables de Chine. La valeur de marché actuelle de l'entreprise avoisine les 755 milliards de dollars.

3 - BAIDU

Moteur de recherche numéro 1 en Chine, Baidu comptabilise environ 80% des requêtes. L'entreprise s'est développée en regroupant de nombreuses fonctionnalités comme Tieba (forum de discussion) ou encore

[10] Business to Business ou activités commerciales nouées entre deux entreprises

Baike (encyclopédie en ligne). De plus, Baidu propose un service de vidéo à la demande via sa filiale iQiyi. Ce service représente un quart de ses revenus. L'entreprise mise aujourd'hui sur l'Intelligence Artificielle (IA), notamment celle appliquée à la voiture autonome et aux assistants personnels, les fameux *bots* (Siri, Alexa, Cortana…).

4 - XIAOMI

Entreprise d'électronique et d'informatique spécialisée dans la téléphonie mobile, Xiaomi, fabrique tout type d'équipements (tablettes, écouteurs et casques, routeurs) et d'objets connectés (bracelets et équipements pour maisons). Dans le domaine des smartphones, Xiaomi a supplanté Apple en 2021 avec 13,5% des parts du marché mondial, pour devenir n°2 derrière le Coréen Samsung.

II - LES MODES OPÉRATOIRES DES GÉANTS DU NUMÉRIQUE

Les mastodontes du digital ont quasiment tous le même mode opératoire dont le mantra serait «phagocyter et neutraliser». D'abord, ils passent un contrat avec un acteur du secteur cible (partenariat, contrat de service), puis, ils étudient le mode de fonctionnement du secteur considéré (chaîne de valeurs, technique, process...), ensuite, ils phagocytent le partenaire et pour parachever le processus, ils le neutralisent en créant un lien de dépendance voire de monopole dans le secteur cible.

Ce mode opératoire n'est pas sans rappeler la stratégie dite du criquet. Les maîtres d'Internet restent dans un secteur tant qu'il y a des opérateurs à s'offrir puis, quand l'écosystème est pieds et poings liés ou supprimé, ils changent de secteurs, tuant toute véritable concurrence sur leur passage. Un mode opératoire que théorise Salim Ismail[11], ancien vice-président de Yahoo et depuis 2020, chargé du développement mondial de Singularity University «*la concurrence est une idéologie qui déforme notre pensée*».

[11] *La fin de l'homme. Les conséquences de la révolution numérique*. La table ronde, 2002.

A - L'ACQUISITION ABUSIVE DES START-UP INNOVANTES

L'empire des GAFAM est bâti sur des centaines d'acquisitions de start-up et d'entreprises. Ces pôles dominants du numérique se déploient à peu de détails près de la même manière. A partir de leur cœur de métier: le e-commerce pour Amazon, ou la recherche web pour Google, ils s'étendent sur d'autres terrains d'une façon tentaculaire par le biais d'acquisitions

En 2020, Facebook, Apple, Microsoft, Google et Amazon ont à eux seuls acquis plus d'une douzaine de start-up spécialisées en IA (Intelligence Artificielle) pour améliorer leurs produits existants et s'ouvrir vers de nouveaux marchés. Depuis 2020, le total de start-up rachetées par les GAFAM est de soixante-quatorze, dont vingt-sept par Apple, Google suit avec quinze acquisitions.

Amazon est passé **d'une simple librairie en ligne à la plus grande plateforme** de e-commerce unifiée du monde. Pour se hisser au sommet, elle a racheté plusieurs dizaines d'entreprises de ce secteur telles que Zappos (entreprise de vente de chaussures en ligne). La firme de Jeff Bezos est aussi devenue **un acteur majeur du commerce alimentaire** en rachetant Whole Foods Market pour 13,7 milliards de dollars. Elle s'est aussi lancée dans le domaine de l'IoT (Internet of Things) en acquérant des entreprises de sécurité domestique ou de routeurs. Depuis 2012, Amazon s'est offert **de nombreuses start up de Cloud Computing**. Sa plateforme AWS (Amazon Web Services) écrase la concurrence dans le domaine de l'industrie du Cloud. Elle est également dans les secteurs de la robotique, de la domotique ainsi que de la santé et des véhicules autonomes…

Apple a racheté de nombreuses entreprises dans le domaine de l'automatisation logicielle, des assistants virtuels ou des capteurs de santé. En 2010, elle a acheté **Siri qui était à l'origine développé par le *Department of Defense* (Etats-Unis).** Depuis 2013, la firme que dirige Tim Cook a acquis 14 entreprises d'intelligence artificielle, de reconnaissance faciale ou de *Machine Learning*. Dans sa gibecière, on retrouve des entreprises à forte croissance. On peut citer l'exemple de **Beats acquis pour seulement 3 milliards de dollars en 2014**, lui ayant permis de se lancer dans le secteur du streaming musical avec Apple Music et de

concurrencer Spotify. Sur les six premiers mois de 2021, Apple a pris possession de 25 entreprises.

Google est loin d'être en reste. De Google Docs à Google Earth, presque tous ses produits découlent des acquisitions. En juillet 2005, sept ans seulement après sa création, **l'équipe de Sergueï Brin et Larry Page s'offrait Android** et son système d'exploitation mobile pour 50 millions de dollars. Pour **concurrencer Microsoft sur le créneau des applications d'entreprise**, elle n'a pas hésité à acquérir des start-up déjà bien implantées. C'est ainsi que Writerly est devenu Google Docs et Tonic Systems rebaptisé Google Slides. En 2007, Google s'entiche du streaming vidéo et achète YouTube pour 1,6 milliard de dollars. Même ses revenus publicitaires découlent d'une technologie acquise au milieu des années 2000 avec l'achat de la startup DoubleClick. Depuis 2007, **Google s'est offert plus d'une trentaine d'entreprises d'Intelligence Artificielle.** C'est ce qui lui a permis d'enrôler les plus grands chercheurs en Intelligence Artificielle, comme Demis Hassabis dont l'entreprise DeepMind fut acquise en 2014. Google s'active également **dans le secteur du Cloud pour concurrencer Amazon et Microsoft**. Il a notamment racheté Alooma, Looker, Elastifile et CloudSimple en l'espace de six mois en 2019. Le secteur de **la cartographie numérique est détenu à 80% par Google**. En plus de développer son outil Google Maps, la firme a absorbé son principal concurrent Waze en 2013.

Enfin, Facebook a peut-être acheté moins d'entreprises que ses rivaux, mais elle a réalisé l'acquisition la plus chère parmi tous les GAFAM en s'offrant **WhatsApp pour 19 milliards de dollars en 2014.** Deux ans plus tôt, elle avait acheté Instagram pour 1 milliard de dollars. Elle a aussi tenté de s'emparer de Snapchat pour 3 milliards de dollars, se heurtant au refus du fondateur Evan Spiegel. L'histoire du réseau social de Mark Zuckerberg commence d'ailleurs par une acquisition. Dès 2005, la firme a acheté **AboutFace qui détenait le nom de domaine «facebook.com».** Et récemment, Facebook s'est lancée sur le marché de la réalité virtuelle en achetant **Oculus pour 2 milliards de dollars.**

Ces acquisitions ont permis aux GAFAM de **s'offrir de précieux brevets et d'ingénieurs très brillants.** C'est ainsi que des produits phares ont pu voir le jour, comme Google Docs ou iTunes. Dans certains cas, il

s'agissait plutôt d'une façon d'éradiquer toute concurrence et les entreprises acquises ont littéralement disparu.

B - LES CONDITIONS DE VENTE OPAQUES

Les géants du numérique ont aussi en partage la complexité de leurs conditions générales de vente. Globalement, elles sont extrêmement opaques voire illisibles. Le consommateur ou le client n'a d'autre choix que d'y souscrire, faute de quoi il perd le service, ses documents, courriels, photos… Les clients et utilisateurs évoquent des formes de verrouillage dues à des conditions de sortie techniquement dissuasives et très onéreuses. D'une manière générale, on déplore un **manque de transparence sur leurs pratiques**, ou, plus grave, une duplicité.

LE PROFILAGE

Depuis 2010, l'humanité produit autant d'information en deux jours qu'elle ne l'a fait depuis l'invention de l'écriture, il y a 5 300 ans. 98% de ces informations sont aujourd'hui consignées sous forme numérique. Tout y passe: photos de famille, musiques, documents administratifs, films, recettes de cuisine, poèmes, romans... Une mise en données du monde qui permet de paramétrer la vie humaine dans ses moindres détails. Dans leur ouvrage intitulé *L'homme nu. La dictature invisible du numérique*, Marc Dugain et Christophe Labbé (2016)[12] sonnent le tocsin sur l'apparente gratuité des services qu'offrent les GAFAM: «Si en apparence l'utilisation de Google ou de Facebook semble gratuite, ces entreprises servent d'interface à de nombreux services». En effet, elles collectent les données concernant nos préférences, centres d'intérêt et autres, pour les revendre à des fins publicitaires. Une méthode particulièrement rémunératrice, car ces informations permettent de cibler avec une précision chirurgicale un profil d'utilisateur et donc de réaliser un impact bien plus efficace sur le plan commercial. Leur monopole leur permet de fixer les prix de ces publicités numériques ou de mettre en valeur leurs propres produits.

[12] M. Dugain et C. Labbe, *L'homme nu*. *La dictature invisible du numérique*, Paris, Robert Laffont-Plon, 2016, Page 23

Microsoft, Apple et maintenant Google imposent leurs logiciels aux utilisateurs de leurs produits. Des méthodes qui laissent peu de place à la concurrence pour se faire une place. Les géants d'Internet ont en commun de recueillir des données permettant d'orienter les publicités des marques vers des acheteurs potentiels, en fonction de leur profil socio-économique. Cette «datification» qui frise le profilage est certes de notre fait, par notre présence en ligne, nous générons volontairement des données. Nous produisons également des données à notre insu via nos contacts, on parle alors de *shadow profiling*, même si nous ne sommes plus connectés, en croisant nos traces laissées sur le Web et nos accès mobiles.

III - LA SOUVERAINETÉ NUMÉRIQUE

Ne crions pas pour autant haro sur ces géants du numérique et les Etats dont ils dépendent. Ils ont pris la place que nous avons voulu leur laisser, telle est la loi de la nature. En ne rencontrant aucune résistance, ils ont occupé le terrain, profitant d'un défaut d'acculturation et de formation. Nous devons toutes et tous reprendre les rênes de nos données et élaborer une véritable stratégie en la matière. Les choix technologiques, nous ne le répéterons jamais assez, sont des choix politiques. Saisissons-nous du sujet. Non, nous n'avons pas le choix entre la Chine ou les Etats-Unis ! Nous devons créer une troisième voie: celle de la souveraineté numérique. Nous avons les moyens de construire notre indépendance technologique et notre souveraineté numérique au niveau national et sous-régional. Nous avons tous les atouts et talents pour que le «monde de demain» ne soit pas un concept marketing supplémentaire ni l'ère du vide pourvoyeuse de désastres économique, écologique et social.

CONCLUSION

La **croissance exponentielle des géants du numérique et leur outrageuse domination** du marché ont d'importantes conséquences pour les internautes, pour les concurrents, et plus généralement pour

l'architecture entière d'Internet. Ces acteurs dominants du cyberespace ont **le pouvoir d'éliminer toute concurrence** pour s'assurer l'oligopole, et n'hésitent pas à le faire. Ceci passe par l'acquisition des start up à succès et des nouveaux arrivants, à la manière dont Facebook a acquis Instagram et WhatsApp. Ils peuvent aussi **promouvoir leurs propres produits et services**, à l'instar de Google via les résultats de son moteur de recherche. Cette stratégie impérialiste réduit fortement la diversité dans le domaine du numérique. En conséquence, **de nombreuses voix se lèvent face à cette hégémonie**. Depuis des années, ces maîtres d'Internet sont accusés de pratiques anticoncurrentielles et font l'objet de nombreux procès en justice, d'enquêtes ou même de sanctions par les régulateurs du marché et les gouvernements des différents pays.

On leur reproche aussi de collecter sans fin des informations sur les internautes. À l'heure où **le Big Data est considéré comme le nouvel or noir**, ces données massives représentent une fortune dont la véritable valeur ne peut être mesurée. Elles représentent aussi et ce n'est pas le moins inquiétant, une menace pour la vie privée.

BIBLIOGRAPHIE

1 Anderson C. *Free ! – Entrez dans l'économie du gratuit*, Pearson Village mondial, 2009, 312 pages

2 Dugain M. et Labbe C., *L'homme nu. La dictature invisible du numérique*, Paris, Robert Laffont-Plon, 2016, 197 pages.

3 Lefilliatre J., «Publicité: Google et Facebook tournent autour du spot», *Libération* du 22 février 2017 à 19h46. Disponible à: https://www.liberation.fr/futurs/2017/02/22/publicite-google-et-facebook-tournent-autour-du-spot_1550324/

4 Montesquieu, *De l'esprit des lois*, Genève, Barillot et fils, 1748, 564 pages

5 Richaud N., «Pour la première fois, le numérique s'arroge plus de la moitié du marché publicitaire en France», *Les Échos*, 7 décembre 2020. Disponible à: https://www.lesechos.fr/tech-medias/medias/pour- la-premiere-fois-le-numerique-sarroge-plus-de-la-moitie-du-marche- publicitaire-en-france-1271724

6 Tessier M. et Baffert M., «La presse au défi du numérique», rapport au ministre de la Culture et de la Communication, 2007

7 Wolf M., «Le nouvel âge de l'automatisation», *Les entretiens du nouveau monde industriel*, décembre 2013

COMMUNICATION DE DEFENSE ET DE SECURITE A L'ERE DE LA LIBERALISATION DU CYBERESPACE

Cyrille Serge ATONFACK NGUEMO
Capitaine de Vaisseau
Chef de la Division de la Communication, MINDEF

INTRODUCTION

Parler de **«La Communication de Défense et de Sécurité à l'ère de la libéralisation du cyberespace»**, revient à expliciter les tenants et aboutissants d'une conflictualité dérégulée dans sa forme, globale dans l'espace et permanente dans le temps. Une conflictualité dérégulée parce qu'à l'instar de l'art de la guerre qui a ses us et coutumes dont la plupart sont contenus dans les règles d'engagement ou d'ouverture du feu, la Communication en tant que discipline dispose de règles qui lui sont propres, notamment d'éthique et de déontologie. Et tel l'art de la guerre dont elle épouse, voire influence les contours, la Communication recourt à des procédés offensifs, défensifs, d'esquive, de ruse, et de plus en plus, de perfidie, quoique cette dernière soit sur le plan éthique strictement prohibées.

Une conflictualité globale, en ce qu'elle intervient aussi bien dans toutes les dimensions de notre planète, voire au-delà, que dans tous les domaines de l'activité humaine. En effet, la transversalité de la Communication est telle que cette dernière est immanente à toute action, ce dès la conception de son intention, transversalité et immanence étant mues par le désir de faire connaître, faire accepter, promouvoir ou défendre un concept

intellectuel, un projet de réalisation, ou un bien matériel ou virtuel.

La conflictualité communicationnelle est également permanente dans le temps et ce, dès les débuts de l'existence humaine. A ce sujet, la fameuse querelle biblique sur l'utilité ou non de manger du fruit de l'arbre de la connaissance du bien et du mal est illustrative à plus d'un titre.

Puisque nous en sommes à une sorte de clarification des concepts, abordons deux notions clés de notre intitulé, à savoir la libéralisation et le cyberespace. Entre autres définitions contenues dans les dictionnaires de la langue française, la libéralisation renvoie au fait d'être favorable aux libertés individuelles. En somme, cette attitude vise à réduire le rôle de l'État, en mettant fin aux monopoles, et en ouvrant tous les domaines à la libre concurrence. Toujours selon les dictionnaires de la langue française, le cyberespace est une étendue immatérielle, impalpable et sans frontière où s'échangent une quantité incommensurable de données numériques, notamment par le truchement du Web, l'Internet, le multimédia.

Donc, en faisant un tout de la liberté d'accès et de l'immatérialité du terrain de manœuvre, et au vu des conséquences négatives, avec entre autres celle de favoriser une asymétrisation de la conflictualité communicationnelle, nous pouvons conclure que la libéralisation du cyberespace s'apparente à l'ouverture de la boîte de Pandore, avec son champ des possibles, bien entendu, y compris son tropisme prononcé pour l'inconnu et le travestissement. Il est en effet constant que les actuels outils de l'information et de la communication sont devenus les supports par excellence de la propagation d'une idéologie belligène et déshumanisante, laquelle se traduit par des actes, de plus en plus nombreux, de violence physique, verbale, d'inversion de la morale, et de contestation des prérogatives de l'Etat.

De notre part, ceci n'est point une réfutation d'une disposition légale favorisant l'essor des échanges et de la science, mais une simple constatation de quelques-uns des effets induits par l'usage malsain qui en est fait. C'est dans cet environnement communicationnel dérégulé, agressif et substantiellement pollué que doit être déployée la Communication de Défense et de Sécurité.

I - DE L'OBLIGATION ET DES ENJEUX DE LA COMMUNICATION

Nous vivons, et chacun peut le constater, dans une société de plus en plus conquise par le pouvoir du son et de l'image. Avec la mise à disposition de technologies communicationnelles de plus en plus faciles à manipuler, toute personne, où qu'elle se trouve sur la planète, peut concevoir, diffuser et recevoir toutes sortes de données relatives à ses besoins. Toutefois, si le rythme et la multiplicité des échanges y gagnent en célérité et opportunités, ceci se fait, très souvent, au détriment du mieux-être tant espéré, la vague transactionnelle pluridimensionnelle globale agissant comme un catalyseur de rivalités, et un exhausteur du désir de renversement des piliers de la normalité sociale.

Compte tenu de sa capacité de mobilisation, la communication se révèle en effet aussi puissante que la poudre et le canon. L'histoire des conflictualités lointaines ou récentes, inter ou intra étatiques, armées ou pacifiques, révèle l'influence capitale de la communication sur le cours des événements que celle-ci est susceptible d'influencer au point d'en changer le cours.

Les idées suprématistes, les appels à la résistance, les mouvements révolutionnaires ou séditieux ne doivent leur impact qu'à l'usage massif des moyens modernes de communication. La propagande nationale-socialiste des années 1930, l'appel du 18 juin 40, la Révolution culturelle, les radios Okapi et Mille Collines, le matraquage publicitaire et les effets de foule induits sont illustratifs de la portée mobilisatrice des supports de communication.

En restant au plus près de nos réalités, celles et ceux qui s'intéressent aux crises sécuritaires dans les régions administratives de l'Extrême-Nord, du Nord-Ouest et du Sud-Ouest du Cameroun, je sais que vous en êtes, étant donné que les questions de défense et de sécurité sont de votre compétence, celles et ceux-là disions-nous, ont pu observer, voire expérimenter les effets néfastes d'une communication tronquée sur les populations desdites régions.

Sur la seule base de narratifs fictifs, exagérés ou déformés à partir de

faits anodins, certaines de ces populations en sont venues à manifester soit de l'indifférence, soit de la méfiance, soit carrément de la défiance vis-à-vis de tout ce qui représente l'autorité légale.

A titre d'exemple, l'école républicaine a été dépeinte par d'aucuns comme un temple de la déviance, pour d'autres comme un instrument d'asservissement linguistique: la destruction des ponts sur des voies d'eau passait pour être une mesure de protection destinée à empêcher l'occupant de reprendre pied sur les territoires libérés: une opération d'extraction et de neutralisation d'engins explosifs improvisés posés sur une route par des terroristes devenait un minage de route par les militaires, etc. Et nous ne parlons même pas des messages d'incitation à la haine, encore moins des appels à la désobéissance civile ou à l'insurrection armée, des campagnes de dénigrement des forces de maintien de l'ordre. L'on peut y ajouter toutes sortes d'imputations visant à décliner des responsabilités, et même des accusations préventives, destinées, à la manière de prophéties auto-réalisatrices, à attribuer à l'autre la responsabilité des crimes que l'on projette de perpétrer soi-même. Tous ces messages sont véhiculés par les autoroutes de l'information.

Sur ce point, le Professeur Kingsley Lyonga Ngange[1] est très explicite: "*Spin room propagandists also known as 'internet generals'...have made frantic efforts to disinform Cameroonians and frame the military as:*

- *People who burn homes of innocent civilians*
- *Enemies of the English speaking population*
- *Forces of occupation*
- *Colonial forces of La Republique*
- *Brutal and aggressive forces*
- *Collectors of 500 frs (bribe in several Police-Gendarmerie Checkpoints), etc".*

Dans cette entreprise de formatage des perceptions à l'encontre des institutions légales, l'on a affaire non plus à de simples usagers ou contradicteurs proposant des sources alternatives d'informations, mais à de

[1] K. Lyonga Ngange, Ph.D. ''Dealing with misinformation and disinformation as weapons of war in Cameroon: what way forward for Defence Forces?'' *Honneur et Fidélité*, décembre 2021, pp 88-91.

véritables combattants du cyberespace qui entretiennent avec des images et surtout des mots, une atmosphère délétère se traduisant par de nombreuses et indicibles violences armées sur le terrain.

Au nombre des combattants du cyberespace, il y a bien sûr les Etats et les organismes qui leur sont peu ou prou rattachés, il y a les organisations internationales et non gouvernementales, et bien d'autres acteurs privés agissant en collectivité ou individuellement. L'on note aussi une dissymétrie qualitative et quantitative en termes de moyens déployés, dissymétrie pas toujours en faveur des acteurs étatiques. C'est ainsi que certaines organisations privées parviennent à se procurer des images satellitaires sur des théâtres d'opérations, alors qu'elles demeurent hors de portée de bien des Etats. D'autres encore parmi ces organisations ont atteint un niveau d'influence tel qu'elles peuvent exiger et obtenir la fermeture d'un compte étatique sur la toile.

Pour les organes de Défense et de Sécurité considérés de manière instinctive ou un tant soit peu objective comme étant les bras séculiers d'une autorité légale castratrice et impitoyable, le principal défi posé par la libéralisation de l'accès au cyberespace est celui de la crédibilité à bâtir, préserver ou reconquérir.

1.1 - DE L'OBLIGATION DE COMMUNIQUER

Pourquoi communiquer, lorsqu'on a pour réputation d'être une grande muette ? A priori, ceci peut sembler ressortir du paradoxe: pourtant il n'en est rien. D'abord, une petite clarification de cette locution nominale s'impose. Le concept de Grande muette accolé aux instruments de force de l'Etat, est une périphrase utilisée en France pour désigner l'armée et ses membres qui, sous la Troisième république, n'avaient pas le droit de vote. Encore aujourd'hui, ils ont, en principe, l'interdiction d'exprimer des opinions sur des sujets sensibles, sociétaux et politiques.

Nonobstant, Olivier Forcade[2] nous apprend que *''Les modes d'expression publique des militaires d'active, inéligibles et privés progressivement de droit de vote de 1872 à 1945, sont déterminés par les principes d'apolitisme et de subordination complète du pouvoir militaire à*

[2] O. Forcade, Les murmures de la ''Grande Muette'' sous la Troisième République. *Editions de la Sorbonne*, 1999, pp 507-519.

l'autorité du gouvernement légal, supposant l'obéissance absolue et le devoir statutaire de réserve des militaires". Or, en dépit de la permanence de ce «*cantonnement juridique»* des armées sous la Troisième République, la»*Grande Muette»* a déployé une stratégie de prise de parole très originale dont l'étude relèverait de la sémiologie. Récurrente, codée, elle a pour enjeu d'émettre des signaux forts à destination des pouvoirs politiques et d'adresser des messages aux opinions publiques tout en respectant les apparences de la morale militaire de silence et neutralité revendiquée.

En gros, l'armée ne s'implique pas dans la politique, mais elle émet des signaux et des messages, ce qui revient quand même à se prononcer, donc à parler. Nous voici en plein dans la polémique. Au point où Georges Lebouc[3] pouvait écrire que Jadis, l'armée était appelée la grande muette. Aujourd'hui, elle parle, et c'est pour débiter du politiquement correct. Laissons-là ces querelles d'idéologie et de principe, pour nous attarder sur la raison d'être d'une communication de Défense et de Sécurité.

En fait, les forces de maintien de l'ordre en tant qu'instrument de matérialisation de la puissance de l'Etat, se trouvent dans l'obligation de porter elles-mêmes l'information nécessaire à la compréhension de leurs intentions ou de leurs actions, à titre préventif, explicatif ou justificatif. En plus d'être un signe d'appartenance à une famille dont elles partagent le quotidien, l'expression directe des forces de maintien de l'ordre est le meilleur moyen pour elles de susciter l'adhésion principalement des populations, ce second degré de légitimation étant, à la suite de la légitimation institutionnelle, le facteur déterminant de la réussite des actions futures.

Au final, cette démarche permet à la fois de se concilier les faveurs des décideurs ou des leaders d'opinion, de consolider l'esprit d'interdépendance avec les populations, et d'éviter des incompréhensions susceptibles d'émaner d'une interprétation erronée ou une distorsion délibérée de la part de vecteurs insuffisamment accoutumés au microcosme de la sécurité. D'ailleurs, il est couramment admis que si vous ne parlez pas de vous-même, quelqu'un d'autre s'en chargera. Et pas de manière avantageuse forcément.

[3] G. Lebouc, Parlez-vous le politiquement correct ? 2007.

1.2 - DES ENJEUX DE LA COMMUNICATION

Les enjeux de la Communication de Défense et de Sécurité sont ceux d'Adhésion, d'Image, d'Influence et de Société. Ils sont à l'image du contexte d'évolution qui est celui, et il faut se l'avouer, des opérations de maintien permanent de l'ordre et la paix, un contexte tellement fragile si ce n'est fragilisé, qu'il est susceptible de dégénérer à tout instant en une crise que la Communication pourrait contribuer sinon à prévenir, du moins à en atténuer la gravité. Evidemment, il s'agit de trouver les justificatifs d'une action parfois considérée comme une intrusion cognitive.

II - DU COMMENT COMMUNIQUER

Comment communiquer relève à la fois du style du discours et des moyens techniques de sa diffusion. En matière d'opération d'influence auprès des instances diplomatiques ou de l'opinion internationale, la Communication de Défense et de Sécurité devrait refléter autant le professionnalisme des forces de maintien de l'ordre que souci des pouvoirs publics en matière de respect des Droits de l'Homme.

S'agissant de l'opinion interne, la Communication devrait tenir le langage de la proximité, la clarté, et d'engagement des forces de maintien de l'ordre à venir à répondre de manière appropriée à la cause d'insécurité.

Donc en fonction des cibles et pour les mêmes faits ou perspectives, la Communication adoptera des angles d'approche et des niveaux de langage différents dans l'optique d'aider l'institution communicante à:

- présenter la meilleure image d'elle-même auprès de ses cibles. C'est assez souvent que les protagonistes d'une crise parviennent à diaboliser les forces maintien de l'ordre, les faisant passer soit pour des forces de répression, d'invasion ou de prédation, soit pour des soutiens à l'une ou l'autre des factions, dans le cas d'une crise intercommunautaire. D'où la méfiance ou pire, le rejet de la part des populations;
- gagner en influence auprès des autorités administratives, des personnalités politiques, des chefferies traditionnelles, des leaders religieux, de la société civile, d'observateurs étrangers. Il s'agit de

les persuader de comprendre, intégrer, justifier et promouvoir les objectifs poursuivis par les forces de maintien de l'ordre;

- susciter l'adhésion des chefs de factions, des intellectuels, des médias et autres faiseurs d'opinion. Une action mal comprise par cette catégorie d'acteurs sociaux fera l'objet d'une présentation tout autant erronée que dangereuse. Les campagnes de dénigrement, les mouvements d'humeur des populations, la recrudescence de la violence, les attaques ciblant les personnels des forces de maintien de l'ordre en sont la preuve;
- rassurer les promoteurs économiques. Le maintien, la reprise ou le renforcement de l'activité économique étant des marqueurs de la continuité de l'Etat, il s'agit d'inciter les acteurs économiques à poursuivre leurs activités, en mettant en exergue les capacités de l'Etat à assurer leur sécurité;
- susciter un sentiment de sécurité et de sérénité au sein des populations. Des populations se sentant en sécurité seront moins portées sur des actes d'autodéfense ou de survie généralement violents. Aussi les actions à mener se doivent-elles d'être bien expliquées et bien menées, autant que possible en partenariat avec les bénéficiaires;
- recueillir le sentiment général par sondage de l'opinion afin de mieux répondre aux attentes;
- promouvoir le retour de la situation d'avant crise, un enjeu sociétal dont l'atteinte n'est possible qu'avec l'assentiment et la collaboration des populations;
- promouvoir de bonnes relations avec les populations des Etats riverains, pour éviter des actes de prédations presque toujours susceptibles de représailles.

En gros, la Communication aura pour rôle de valoriser les initiatives des Forces de Défense et de Sécurité, en les accompagnant de l'intérieur, et en les présentant de la manière la plus avantageuse à l'extérieur. Ce qui revient à investir le champ de bataille communicationnel.

2.1 - DES MOYENS DE LA COMMUNICATION

Pour atteindre ces enjeux d'***Adhésion***, d'***Image*** et d'***Influence*** qui sont autant d'objectifs de choix, la Communication peut se servir de tout ou partie de la panoplie des supports disponibles, à savoir:

- les supports écrits (journal périodique, tracts, dépliants, affiches, gadgets, etc.);
- les supports audiovisuels (programmes radiophoniques, photographies, documentaires télévisuels, sketches, etc.);
- l'Internet et/ou les réseaux sociaux (Facebook, Twitter, Whatsapp, Instagram, Linkedin, etc.)
- le contact physique (campagnes de sensibilisation, promotion de rencontres sportives, séances de socialisation tel l'investissement humain sur des projets communautaires, éducation à la citoyenneté, diplomatie de l'oreiller, etc.).

Les institutions en charge de la Défense et la Sécurité nourrissant l'ambition d'atteindre l'ensemble, sinon la majorité des protagonistes d'une crise, étant donné que la crise est une situation immanente au fonctionnement de toute entité organisée, se doivent de mettre en œuvre une communication adaptée à ses diverses cibles, cohérente dans son message, variée dans sa présentation et permanente dans le temps. Ceci est un impératif en vue de l'atteinte des objectifs que sont la ***sécurisation*** des populations, la ***restauration*** de l'autorité de l'Etat et la ***prévention*** de la résurgence d'un conflit.

2.2 - DES ARTICULATIONS DE LA COMMUNICATION

Le manque notoire de proactivité et de promptitude qui la caractérise contraint la Communication de Défense et de Sécurité à presque toujours agir de manière réactive, après que le champ en friche de la réceptivité des cibles aura été labouré par toutes sortes d'informations, dorénavant difficiles à remplacer. Il est vrai que contrairement aux autres compétiteurs combattants de la sphère cybernétique jouissant de la plus grande liberté de manœuvre à l'échelle individuelle, la Communication de Défense et de Sécurité évolue dans un cadre plus restrictif, faisant exigence de vérification, de contextualisation, de certification et d'habilitation avant

diffusion. Une élongation procédurale à tout le moins préjudiciable à l'atteinte des objectifs poursuivis par les institutions émettrices.

Un palliatif à cette hyper centralisation de la Communication de Défense et de Sécurité consisterait en une espèce de dénivellement sur l'échelle de la prise de décision. Il ne s'agit pas de créer une nouvelle architecture, notamment dans les commandements territoriaux ou les services extérieurs qui ont tous prévu des services de communication. Il s'agit de leur ouvrir de plus larges perspectives d'action afin de permettre auxdites structures de réduire les délais de latence entre la survenue d'un événement les concernant, et la communication officielle qui en est faite. Il s'agit enfin, de sortir la Communication de Défense et de Sécurité de sa routine événementielle officielle, pour l'amener vers la couverture des activités de socialisation.

A cet effet, il sera digne d'intérêt de donner le plus grand écho possible aux actes de sécurité pure, à l'instar de la neutralisation d'un groupe de terroristes, ou l'arrestation de malfrats, mais beaucoup plus encore à la distribution de vivres ou de médicaments à des communautés nécessiteuses. Dans le cas d'espèce, l'usage de langues locales est vivement conseillé.

AU NIVEAU STRATÉGIQUE

Il peut s'avérer nécessaire de créer, à défaut d'une Composante, à tout le moins une Section Communication chargée de concevoir, de mettre en œuvre et de coordonner les activités de ce ressort. Cette Composante/Section pourrait se voir chargée de:

- la création et l'animation d'un programme radiophonique quotidien ou hebdomadaire dans les langues officielles;
- l'insertion d'espaces de sensibilisation dans les médias nationaux ou régionaux;
- l'animation d'un Point focal Communication pour les médias;
- la tenue périodique de points de presse (périodicité à déterminer);
- l'organisation de voyages de presse pour un plus grand retentissement national et international;
- la rédaction, la lecture, la distribution et la diffusion des communiqués de presse.

AUX NIVEAUX OPÉRATIF ET TACTIQUE

En dehors des descentes ponctuelles des personnels de l'Etat-major sur le terrain, il reviendra aux échelons opératif et tactique, en collaboration avec les médias locaux, d'élaborer des programmes de communication dans les langues locales les plus usitées et portant entre autres sur les nouvelles de la caserne, les activités civilo-militaires, les actions d'éclat, les opinions et vœux des populations, etc.

Ce faisant, l'on va migrer d'une Communication de Défense et de Sécurité centrée sur le pouvoir et les décisions de l'Etat, vers une Communication sociale de Défense et de Sécurité plus accommodante pour les populations, principales cibles de la bataille communicationnelle qui fait rage dans le cyberespace.

Tant de détails et d'insistance sur les actions de socialisation, entendues dans le jargon militaire comme étant des opérations autres que la guerre, se justifient par la valeur critique des perceptions, pour le gain desquelles les acteurs de la belligérance se livrent une bataille acharnée dite ''guerre des cœurs''. L'inclination logique ou sentimentale des cœurs est en effet un des facteurs décisifs de la réussite de toute opération, fût-elle humanitaire ou mieux, sécuritaire, surtout par ces temps de contestation bruyante et violente des exclusivités régaliennes.

2.3 - DE LA SPÉCIFICITÉ DE LA COMMUNICATION INTERNE

Dans l'actuel contexte cyberinformationnel intrusif, corrosif et dolosif se caractérisant par un matraquage à outrance de l'émotionnel, concevoir et déployer une communication uniquement centrée sur des cibles extérieures, fait courir à l'institution communicante le risque d'un découplage d'avec ses propres personnels. En effet, est-il seulement possible de présumer de l'efficacité d'une communication dont les vecteurs ne s'accordent ni sur la vision, ni sur la forme, ni sur les cibles ? On peut poser le problème autrement.

Qu'est-on en droit d'attendre de la part de policiers, de gendarmes et de militaires appelés à remplir une mission vis-à-vis de laquelle ils émettent quelques objections, pour diverses raisons, notamment celles en rapport

avec des liens familiaux, des convenances morales ou intellectuelles, ou encore l'appartenance religieuse ? Au mieux ils s'acquitteront du service minimum, au pire l'on assistera au phénomène de *crosses en l'air*, autrement dit, à un refus d'obéissance, voire à une mutinerie. Et c'est l'objectif des actions adverses de communication.

A titre d'illustration, et à la faveur du présent conflit armé en Europe de l'Est, l'on a vu circuler sur les réseaux sociaux, des images de soldats prétendument en détresse, du fait du manque de rations alimentaires, des bataillons entiers en manque de carburant et de munitions. De tels messages n'ont pour objectif que de démoraliser les troupes dont la confiance en la capacité de leur hiérarchie de savoir planifier et conduire une opération se trouve diminuée.

La Communication devrait dès lors servir à dresser des pare-feu cognitifs contre des velléités de démoralisation des personnels. Donc, et de même que cela se fait pour les cibles externes, il s'agira, au préalable d'amplement communiquer en interne, de manière à permettre aux personnels, engagés ou non, d'entretenir une vision globale commune, objective et dynamique de la raison d'être des activités en cours ou à venir, et dont ils pourraient se voir confier la responsabilité de l'exécution.

CONCLUSION

Domaine transversal mis en œuvre depuis le niveau stratégique jusqu'à l'échelon opérationnel, la Communication est autant une indispensable fonction de commandement, que le principal vecteur de mise en perspective avantageuse des actions et intentions de l'institution communicante, notamment auprès des populations dont l'adhésion est vitale pour la réussite des missions. Une intégration de la Communication au chapitre des rubriques cardinales du concept d'opération semble à cet effet nécessaire, ce qui va permettre une préparation des éléments d'information à livrer à l'opinion dans la mesure du possible avant, mais surtout pendant ou sitôt après la fin d'une opération.Sans aller jusqu'à faire recours aux méthodes contradictoires à l'éthique et la déontologie, la Communication de Défense et de Sécurité devrait néanmoins pouvoir forcer le trait sur les exactions perpétrées par les forces d'opposition, ceci pouvant se faire soit de manière directe, soit à travers des extensions.

Au reste, si la Communication demeure pour l'essentiel un moyen de persuasion massive, elle n'en est pas moins un redoutable moyen de coercition. Bien utilisée, elle agit de la même façon que les facteurs de la puissance, notamment l'économie, le militaire, la culture, etc. En fonction des cibles et pour les mêmes faits ou perspectives, la Communication adopte des angles d'approche et des niveaux de langage différents. Il s'agit de présenter la meilleure image possible de l'Institution, car c'est assez souvent que les protagonistes d'une crise parviennent à diaboliser les forces engagées dans les opérations de retour à la normalité. D'où la méfiance ou pire, le rejet de la part des populations. Entre autres objectifs de la Communication, il est également question de persuader les autorités administratives, les personnalités politiques, les leaders religieux, traditionnels ou d'associations, de comprendre, d'intégrer et de promouvoir les objectifs de l'action des forces de maintien de l'ordre, dans le but de susciter un sentiment de sécurité et de sérénité au sein des populations qu'ils représentent ou dont ils ont la charge. En effet, des populations se sentant en sécurité sont moins portées sur des actes d'autodéfense ou de survie généralement violents. Aussi les opérations menées par les forces de maintien de l'ordre doivent-elles être minutieusement expliquées avant, pendant, et longtemps après qu'elles soient parvenues à leur terme.

Il s'agit, au final, de susciter l'adhésion, d'entretenir l'image de l'Armée, de gagner en influence auprès des faiseurs d'opinion, voire de faire évoluer les idées reçues de la société. Comme il apparaît très clairement, les enjeux sont importants sur ce terrain rendu traître par une opinion versatile abreuvée de sons discordants.

PANEL 2: MEDIAS SOCIAUX ET NUMERISATION: DILEMME «RISQUE-OPPORTUNITE» SECURITAIRE

LES RESEAUX SOCIAUX, L'INGENIERIE SOCIALE, LE PHISHING, LES FAKE NEWS: ETAT DES LIEUX ET PERSPECTIVES

Françoise EKOLLO
Experte en systèmes d'information, consultante en cybersécurité

Avec l'avènement la mondialisation, on va assister au développement des Technologies de l'information et de la communication, et partant les réseaux sociaux. En marge du caractère vertueux du phénomène mondial, prolifèrent également d'autres phénomènes potentiellement néfastes pour la sécurité à la fois des personnes physiques et personnes morales. Au nombre de ceux-ci, nous pouvons évoquer l'ingénierie sociale, le phishing, les fake news. Pour mieux cerner ces notions, des précisions sémantiques sont indispensables. Aussi, par ingénierie sociale (ou *social engineering* en anglais), il faut entendre l'ensemble des pratiques de manipulation psychologique à des fins multiples (vol, abus, escroquerie, destruction de données, etc.). Quant à l'hameçonnage ou *phishing* en anglais, il s'agit d'une technique frauduleuse qui vise à obtenir des informations privées. Concernant les fake news, l'expression anglaise signifie «fausses nouvelles» et désigne des informations fausses qui souvent sont volontairement truquées. Que signifient ces menaces, qu'ont-elles en commun, comment impactent-elles sur le quotidien des usagers dans leur utilisation des réseaux sociaux ? Et quels sont les moyens pour y faire face ?

Les phénomènes susmentionnés, de par leur spécificité, se déclinent en des menaces contre les données des usagers dans leur utilisation des réseaux sociaux et autres solutions technologiques (I). Et les moyens de prévention et pour y faire face sont de plusieurs ordres (II).

I - FAKE NEWS, PHISHING, INGÉNIERIE SOCIALE: DES MENACES CONTRE LES DONNÉES DES USAGERS DANS LEUR UTILISATION DES RÉSEAUX SOCIAUX ET AUTRES SOLUTIONS TECHNOLOGIQUES

Selon les réseaux sociaux (A) et l'usage qui en est fait par leurs utilisateurs, les facteurs de vulnérabilité sont plus ou moins importants (B). D'où l'on peut noter des fenêtres d'opportunité donnant lieu à la pratique des fake news, du phishing ou de l'ingénierie sociale.

A - AU CŒUR DES RÉSEAUX SOCIAUX

Au gré des développements et prouesses technologiques, les réseaux sociaux naissent tous les jours. En effet, leurs concepteurs repoussent les limites de la technologie pour concevoir des outils qui répondent de plus en plus aux attentes et autres besoins et comportement des internautes et matière de partage et de consommation de l'information. Par réseau social, il faut entendre une plateforme en ligne permettant aux personnes de nouer des relations, de communiquer et d'échanger des informations de divers formats (messages texte, photos, vidéos, etc.). On peut classer les réseaux sociaux selon la typologie suivante :

- Les réseaux sociaux génériques: Il s'agit de plateforme permettant de communiquer et d'interagir sur plusieurs types de contenus: textes, images, vidéos, jobs, publicité, jeu, publicité, commerces. Dans cette catégorie, nous pouvons citer Facebook, Instagram, Twitter, etc.
- Les réseaux sociaux professionnels. Par rapport aux premiers, ils se distinguent de par la qualité des contenus qui y sont échangés. En effet, ladite plateforme est dédiée aux échanges et interactions sur des contenus professionnels. Il s'agit des réseaux sociaux du type de Linkedin, Viadeo, Quora, etc.
- Les réseaux sociaux de partage. Ici, ce qui est partagé est un type

précis de contenus. Il peut s'agir de vidéos, images, musique, centres d'intérêts, etc. Dans ce groupe, l'on retrouve des plateformes comme Youtube, Flikr, Ask, etc.

- Les réseaux sociaux d'entreprise. Comme leur nom l'indique, ces outils sont principalement utilisés pour des interactions au sein d'une entreprise. A titre d'exemple, nous pouvons citer: Facebook at work, Bitrix, etc.

Après cette présentation succincte des réseaux par typologie, il serait intéressant d'insister sur les menaces qui y opèrent et auxquelles les utilisateurs doivent faire face.

B - SPÉCIFICITÉS DES MENACES À L'USAGE DES RÉSEAUX SOCIAUX ET AUTRES SOLUTIONS TECHNOLOGIQUES, FACTEURS DE VULNÉRABILITÉ

Il existe plusieurs types de menaces liées aux données des usagers, qu'il s'agisse des personnes physiques ou morales. Au nombre de celles-ci, nous pouvons citer l'ingénierie sociale, le phishing, les fake news.

Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.). En utilisant ses connaissances, son charisme, l'imposture et le culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité des personnes possédant ce qu'il souhaite obtenir. Les comportements des personnes peuvent avoir des conséquences importantes sur les questions de sécurité de l'information au sein du cyberespace. On peut noter à titre d'exemple: les pertes économiques, la violation et perte d'intimité, la perte de crédibilité et/ou de réputation, la fermeture provisoire ou dépôt de bilan, faillite, Etc. Il existe plusieurs types d'attaques d'ingénierie sociale :

- L'ingénierie sociale humaine (human-based social enginnering): Elle recueille des informations sensibles par interaction. La technique

utilisée est l'imitation (impersonation) et les méthodes employées sont nombreux notamment le dumpster diving, le piggybacking, le reverse social engineering, le tailgating.

- L'ingénierie sociale basée sur le mobile (mobile-based social engineering): elle est réalisé à l'aide d'applications mobiles. Plusieurs moyens employés, notamment des fausses applications de sécurité des mobiles (antivirus), des applications malicieuses de publicité, etc.
- L'Ingénierie sociale informatisée (computer-based social engineering): elle est réalisée à l'aide d'ordinateurs. Plusieurs moyens employés notamment les fenêtres popup Windows, le **phishing**, le **spear phishing, le whaling.**

L'hameçonnage ou *phishing* en anglais est une technique frauduleuse qui vise à obtenir des informations privées. Exemple: *L'escroc prend contact par courrier électronique en faisant croire à sa victime qu'il s'agit d'un organisme de confiance - banque, fournisseur d'électricité, police, etc. - et lui demande la confirmation d'une information (mot de passe, numéro de carte de crédit, code d'accès, identifiant, etc.) Sous peine de lourdes conséquences… Le mail contient alors un lien renvoyant vers un site internet paraissant tout à fait officiel aux yeux de la victime. C'est pourtant une copie faite par l'escroc qui permettra dès lors que la victime aura renseigné les informations demandées de les récupérer pour pouvoir les réutiliser et également avoir accès aux données personnelles de la victime.*

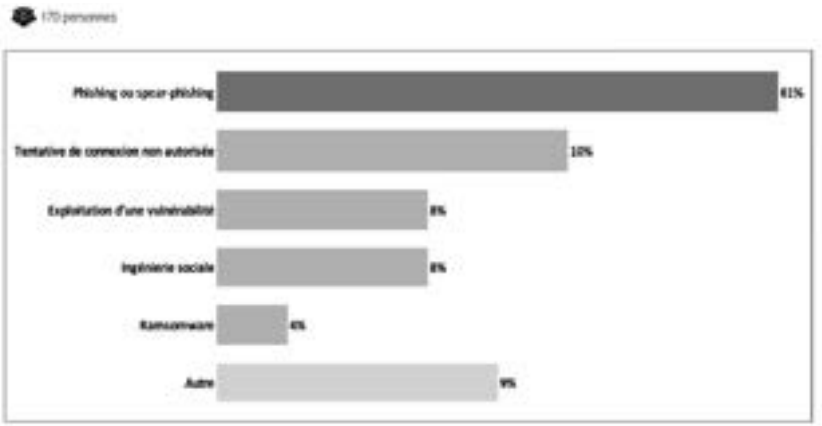
Le **spear phishing** se distingue du phishing. En effet, le spear phishing est une attaque ciblée en l'endroit des individus précis dans une organisation. En comparaison du phishing qui procède par une attaque par envoi de milliers de messages génériques à des adresses ou des personnes de manières aléatoires. Le spear phishing devient aujourd'hui la tendance du fait de l'usage des nouveaux moyens de communications (réseaux sociaux, sites internet, etc…) par les organisations qui fournissent de plus en plus des informations sur leurs activités et leurs personnels.

Le Whaling est similaire au spear phishing avec la différence qu'il est bien plus ciblé encore à l'endroit des personnels de haut niveau (directeurs

de ressources humaines, directeurs financiers, directeurs généraux) qui disposent de hautes responsabilités et détiennent des informations ultra sensibles et confidentielles. Aux Etats-Unis par exemple, selon le FBI les dégâts occasionnés par le whaling entre 2016 et 2019 se sont chiffrés à plus de 26 milliards de dollars avec une augmentation de 100% dans l'intervalle 2018 à 2019. Le *whaling* devient aujourd'hui la technique de phishing la plus prisée par les hackers car bien plus dangereux avec des dommages plus significatifs

S'agissant des fake news, ses objectifs sont également nombreux: par exemple, tromper un lecteur ou alors influencer son opinion pour un sujet particulier. Les réseaux sociaux comme les plateformes web sont un parfait vecteur de propagation d'informations trompeuses (Google news, Facebook, Twitter, etc). Pour s'en prémunir il faut effectuer un travail de journaliste (fact checking) mais pas seulement et, en se posant des questions suivantes mais non exhaustive: L'information est-elle fiable ? Quelle est la source ? Est-elle crédible ? L'information est-elle neutre ? Quel est l'intérêt de la propagation de cette information ? Etc.

Aucun pays n'est épargné par ces attaques. A titre d'exemple, au Cameroun, de nombreuses arnaques sont perpétrées à l'aide des outils informatiques. Ce type de cybercriminalité représente environ 80% des cas de cybercriminalité et a causé une perte estimée à 7 milliards de FCFA depuis 2010. Pareillement, de nombreux usagers sont victimes d'h**ameçonnage**. L'hameçonnage est la tentative frauduleuse d'obtenir des informations ou des données sensibles, telles que des noms d'utilisateur, des mots de passe, des numéros de carte de crédit ou d'autres détails sensibles en se faisant passer pour une entité de confiance dans une communication numérique et représente environ 15 % des cas de cybercriminalité signalés, largement influencé par l'avènement des services ebanking et Mobile Money. Ce type de cybercriminalité a causé une perte estimée à 4 milliards de FCFA depuis 2010: A cet effet, plus de 3 000 réclamations relatives à des escroqueries et phishing reçues depuis 2019 au niveau de l'ANTIC.



Proportion du phénomène en Afrique. Source: Baromètre de la cybersécurité en Afrique 2022. Le CESIA (Club d'Experts de la sécurité de l'Information en Afrique)

De nombreux facteurs favorisant la vulnérabilité aux attaques existent. Au nombre de ceux-ci, l'on peut citer:

- Le principe de confiance de la nature humaine;
- L'ignorance ou la méconnaissance de l'ingénierie sociale;
- La cupidité humaine;
- L'absence de formation sur la sécurité des systèmes d'information;
- L'absence de politiques de sécurité;
- Le manque de formation du personnel;
- L'absence des procédures de sécurité;
- L'absence ou la faiblesse d'un système de sécurité physique;
- L'illusion de la sécurité;
- L'absence d'un système de gestion des identités efficaces;
- La place tertiaire de la sécurité au cœur des traitements;
- L'ouverture des pièces jointes des mails de source inconnue;
- L'ignorance des personnels des techniques d'ingénierie sociale;
- L'absence d'utilisation de l'authentification à plusieurs facteurs;
- L'ignorance des techniques récentes;
- L'absence de mise à jour des antivirus;
- L'absence de protocole de contre surveillance.

II - MOYENS DE PRÉVENTION ET DE LUTTE DES MENACES INTERNES

En matière de prévention et de lutte face aux atteintes contre les données des utilisateurs, on ne le dira jamais assez, la première barrière reste l'usager lui-même et l'usage qu'il fait de sa présence en ligne. En effet, au quotidien, nous avons recours aux réseaux sociaux et autres solutions technologiques qu'il s'agisse de communiquer avec des proches, rechercher ou partager des informations, dans un environnement privé ou professionnel. De par ses usages, nous exposons nos données à des internautes malveillants. De fait, une plus grande vigilance est de mise, dans la gestion des mots de passe, la sécurisation de nos appareils… Cette prudence nous permet nous-même d'être à l'abri des vulnérabilités des réseaux sociaux et autres outils technologiques.

Pour la prévention des menaces internes, c'est-à-dire, une menace pouvant venir du fait de l'espionnage par une organisation concurrente qui peut infiltrer l'organisation cible soit en y envoyant une personne en stage ou en recrutement ou alors en y procédant par connivence avec une personne mécontente) divers mécanismes peuvent être mis en place à l'instar de:

- La séparation et la rotation des rôles et responsabilités;
- La restriction des privilèges;
- Le Contrôle des accès;
- L'audit et gestion des évènements;
- Les politiques légales;
- L'archivage des données critiques;
- La Formation et l'éducation.

De manière globale, la lutte contre les pratiques d'ingénierie sociale et autres fake news, phishing peut se faire à plusieurs niveaux. Dans un premier temps, elle devrait être menée au niveau des comportements des usagers. En effet, il s'agit de mener au sein de la société et notamment de toutes les couches sociales, des campagnes de sensibilisation, d'information et de formation pour une protection optimale de leurs données et notamment pour un usage vertueux des réseaux sociaux et autres produits du web.

S'agissant de la gouvernance des systèmes d'information, il s'agira de mettre un accent sur les directives opérationnelles, la classification des informations, des procédures de réponse face aux incidents, ainsi que des procédures de vérifications avancées dans le cadre du recrutement.

Sur le plan technique, il s'agira de mettre en place une politique du mot de passe, la mise en place de systèmes physiques de sécurité: la mise en place de systèmes de défense au périmètre et à l'intérieur du réseau de l'organisation: la mise en place d'un système d'authentification au moins à deux facteurs, idéalement à multiple facteurs: la mise en place de systèmes d'audit automatisé.

CONCLUSION

L'usage quotidien des réseaux sociaux n'est pas sans vice et vulnérabilités. En effet, personnes physiques et morales ne sont pas à l'abri des vulnérabilités du web. Lesquelles portent atteinte notamment à l'intégrité de leurs données, qu'elles soient personnelles ou professionnelles. Au nombre de ces atteintes, nous avons longuement évoqué les fake news, le phishing et l'ingénierie sociale. En analysant ces menaces, nous avons pu nous rendre compte de la place essentielle qu'occupe l'Homme dans la protection de ses données sur internet et les réseaux sociaux. En effet, si l'option de ne pas y aller reste la meilleure, on ne peut aujourd'hui, dans un monde en pleine mutation, se passer de l'usage des réseaux sociaux. Et leur usage au quotidien n'offre pas une protection maximale.

Passé cette vigilance humaine, le modèle «zéro trust» semble aujourd'hui, également présenter une certaine fiabilité. **«Zero Trust»** est un modèle de sécurité basé sur un processus de vérification d'identité stricte, dynamique et permanente. Le concept d'utilisateurs de confiance et autorisés (concept d'annuaire dans les organisations) n'est plus considéré et ne bénéficie d'aucune confiance. Après une vérification de l'identité de l'utilisateur, son authentification et son autorisation, un tunnel sécurisé crypté avec certificat est établi avec l'application et régulièrement contrôlé avec éventuellement la possibilité de le déconnecter en cas de comportement anormal. Le modèle protège également les applications et utilisateurs contre les menaces avancées sur Internet. Le principe est simple: Zéro confiance aux équipements: Zéro confiance aux données: Zéro confiance aux réseaux: Zéro confiance aux charges de travail: Zéro confiance aux personnes. En un mot, **# Toujours tout vérifier#**

DE LA DEFIANCE DE L'ORDRE WESTPHALIEN A L'IRRUPTION DES SYSTEMES D'ALLEGEANCE CONCURRENTIELS: LA BATAILLE MEDIATIQUE DE LA LEGITIMITE ET DE LA REPRESENTATIVITE

Jean NJOYA
Professeur Titulaire de Science Politique
Vice-Recteur chargé des enseignements, de la professionnalisation et du développement des TIC
Université de Dschang-Cameroun

INTRODUCTION

Le paradoxe qui affirme que l'Etat n'a pas toujours été la seule forme de société politique est vrai. Lorsque les anthropologues actionnent la touche arrière de la machine historique, ils répertorient une palette foisonnante d'organisations politiques[1]. Sous les tropiques, une dichotomie suggestive mais d'une portée sommaire a été même canonisée opérant une distinction entre les «sociétés étatiques» et les «sociétés sans Etat»[2] .

Cette discrète intrusion dans l'Anthropologie de l'Etat[3] - qui n'a pas seulement le brillant du paradoxe-, confirme et conforte un fait mainte fois

[1] Lapierre J. W., *Essai sur le fondement du pouvoir politique*, Publications de la faculté des lettres d'Aix en Provence, Ophrys, 1968.
[2] Pritchard E. E. et Fortes M., *Les systèmes politiques africains*, Paris, PUF, 1964.
[3] Abelès M., *L'anthropologie de l'État*, Paris, Armand Colin, 1990.

refoulé par l'histoire politique: celui de l'inexistence historique de l'Etat hors contexte occidental. Est donc privilégiée, ce que l'on peut appeler la thèse de l '»hexagonalité» de l'Etat pour signifier son origine occidentale[4].

Si nous acceptons cette thèse avec la claire conscience d'en payer le prix, elle nous introduit du reste commodément dans l'idée que les «traités de Westphalie» constituent les fonts baptismaux de la construction d'une société internationale de puissance. En effet, ces conventions clôturent la «guerre de trente ans»[5] et consacrent l'Etat comme sujet et acteur uniques du droit des relations internationales.

Une critique sévère de l'«Ordre westphalien», ne rend toujours pas compte de l'effort consolidé de juridicisation des rapports internationaux: trop besogneuse, elle pointe singulièrement le caractère hégémonique de ce»nouvel ordre européen»[6], aussi bien qu'une sorte de «confessionnalisation» des relations internationales, passant ainsi par pertes et profits, le processus de «civilisation des mœurs politiques» internationales qu'il charrie[7]. Le fait qui assimile l'ordre westphalien à l'émergence d'une civilité internationale bien qu'intermittemment marquée de conflictualité est irrécusable.

C'est, au demeurant, cette conflictualité quasi-permanente qui grève d'illégitimité l'ordre westphalien: qui plus est, il est écorné par une mondialisation disruptive qui rend labiles les frontières territoriales de l'Etat et le shunte dans ses fondements existentiels. Elle offre aux acteurs transnationaux et à la circulation des idées, les possibilités d'une mobilité accrue. L'on serait passé du «monopole dur» des Etats sur les relations internationales à un «monopole souple» ou une véritable foire d'empoigne caractérise les luttes d'occupation de l'espace international par l'Etat et les nouveaux acteurs des relations internationales.

---

[4] Voir Norbert E., *La dynamique de l'Occident*, Paris, Calmann-Lévy, 1973.

[5] C'est une guerre qui a eu lieu de 1618 à 1648, opposant les princes allemands catholiques et protestants. La plupart des nations européennes ont pris part à cette guerre qui a causé près de 7 millions de morts: et, ce sont les traités de Westphalie qui ont mis un terme à ces hostilités.

[6] Blin A., *1648, la paix de Westphalie ou la puissance de l'Europe politique moderne*, Bruxelles, Coll. «Question à l'histoire», 2006.

[7] Elias N., *La civilisation des mœurs*, trad. Fr. 1973, Paris Calmann-Levy, 1991.

Le paradigme des «turbulences» dans la politique internationale proposé par James Nathan Rosenau, exprime mieux cette ivresse de la métamorphose, puisque l'auteur examine les acteurs parties prenantes du système international en soutenant que leur nombre sans cesse croissant engendre une complexité de ce système[8]. L'image d'Epinal surfaite que l'ordre westphalien a investi dans l'Etat, se révèle aujourd'hui être un mythe usé au regard de la défiance qu'inspire ce modèle d'organisation politique. De toute évidence, le système de régulation internationale établi par le texte de Westphalie avait pu garantir un minimum de stabilité dans la conduite des affaires mondiales du moins jusqu'aux années 1950.

Toutefois, cet ordre ne demeure-t-il pas un ordre mythique qui continue d'imposer son magistère d'influence dans le puzzle international ? Ceux qui l'ont pensé autrement ont certainement surestimé le changement «pour mieux forcer la pensée à l'innovation»[9]. La prolifération des acteurs hors souveraineté pulvérise-t-elle complètement ce mythe créateur de l'Etat souverain ?

Notre posture est qu'un monde nouveau qui défie l'ordre westphalien sans le supplanter s'implémente, charriant une altération des identités qui «bifurquent» vers une réorientation des liens d'allégeance, d'autorité et de loyauté qui assujettissaient jusque-là les individus et les groupes sociaux.

Dans cette dynamique, le rôle des médias a été crucial dans la «construction de la réalité»[10] internationale. Les médias comme instruments au service de la politique étrangère est - cela va sans dire - un truisme de la diplomatie classique. Mais son usage quasi-inflationniste dans le «storytelling» induit une orientation belliciste dans les relations internationales. Bien plus, la maîtrise de l'internet constitue un enjeu de puissance complètement étranger à l'ordre Westphalien d'origine.

Notre approche sera historique: il s'agira d'une forme allégée d'histoire

[8] Roseneau J. N., *Turbulence in world politics: A theory of change and continuity*, Princeton University Press, 1990.
[9] Girard M., «Turbulence dans la théorie politique internationale ou James Roseneau, inventeur», RFSP, 1992, 42-4/pp.636-646.
[10] Berger P. et Luckman S. T., *La construction sociale de la réalité*, Paris, Armand Colin, 1997.

immédiate qui juxtapose l'ordre westphalien ancien et sa forme contemporaine émasculée pour mieux apprécier les disruptions subséquentes. Aussi, allons-nous d'abord aborder l'ordre westphalien à l'aune du monopole dur qu'ont exercé les Etats sur les Relations Internationales (I), ensuite, ausculter la fragilisation de cet ordre sous l'effet d'une mondialisation disruptive où les nouvelles loyautés se construisent avec les acteurs hors souveraineté (II).

I - L'ORDRE WESTPHALIEN ET LE «MONOPOLE DUR» DES ETATS SUR LES RELATIONS INTERNATIONALES: DE L'ACCAPAREMENT AUX LINEAMENTS D'UNE EMASCULATON DE SES FONDEMENTS

L'on peut reprocher à notre perspective analytique un retour à «l'histoire d'une fiction»[11]. Concédons toutefois qu'il s'agit d'une fiction agissante, car l'ordre westphalien a créé un «monde des choses»[12] avec ses «effets de croyances». Il a marqué pour longtemps la scène internationale, et a forgé les mentalités «statolatriques». L'on ne pouvait concevoir le fait international autrement que comme le fait de l'Etat. L'on a dans le contexte westphalien des origines, une conception hégémonique de l'Etat logé singulièrement en Europe, largement tributaire des rapports de forces issus de la «guerre de trente ans». L'appréhension du traité lui-même n'est intelligible que si l'historiographie recourt minimalement à la «courte durée»[13] incarnée par la «guerre de trente ans». C'est-à-dire cette Europe avant Westphalie, hantée par le «fantôme impérial et ses tentatives de dominations universelles»[14]: période très marquée par les écrits d'Alighierie

[11] Badie B., *Un monde sans souveraineté: les Etats entre ruse et responsabilité*, Paris, Fayard, 1999,p. 17.
[12] Trentmann (Frank), *Empire of things: How we became a world of consumers, from the fifteenth century to the twenty-first*, Londres, Allen Lane/Penguin, 2016.
[13] Braudel F., *Ecrits sur l'histoire*, Paris, Flammarion, 1986. Certes Braudel s'oppose à cette temporalité qu'il considère comme une histoire évènementielle, mais nous considérons *mutadis mutandi* la guerre de 30 ans comme le point nodal d'un enchaînement historique logique.
[14] Bely L., Le «paradigme westphalien» au miroir de l'histoire: l'Europe des traités de Westphalie», Centre Thucydide,

Dante qui prônait au moyen âge l'avènement d'un souverain unique au monde comme il faut un père à une famille[15].

L'environnement historique de production du paradigme westphalien sera donc fortement marqué par des tentatives de dominations universelles et une «confessionnalisation» des relations internationales[16]. C'est cet ordre des choses que le traité va acter en dotant l'Etat des principes juridiques qui vont consacrer sa puissance subjuguante sur la scène internationale.

A - L'ORDRE WESTPHALIEN: UNE «STATOLATRIE» SUBJUGUANTE DE LA SCENE INTERNATIONALE

L'Etat de l'ordre westphalien n'a pas émergé *ex nihilo*. Sa configuration de l'époque a été le résultat des conditions historiques de sa production. Son affinement ultime est intimement lié à l'idéologie de puissance dominée par l'impérialisme - par ailleurs commun - à toutes les maisons souveraines d'Europe enclines à la capture des monopoles militaire et fiscal, à la recherche des territoires nouveaux, et à la constitution des armées plus fortes.

L'environnement historique de production d'un «paradigme westphalien» augure d'une puissance souveraine de l'Etat que ne pouvait contrer qu'un autre Etat souverain. Il y a donc eu une mutation de l'idée de puissance anarchique à l'idée de puissance encadrée.

1 - L'ENVIRONNEMENT HISTORIQUE DE PRODUCTION DU PARADIGME WESTPHALIEN: DES IMPÉRIALISMES À LA CONSTRUCTION DES SOUVERAINETÉS BORNÉES

La «défenestration de Prague» fut l'étincelle d'une guerre de trois décennies[17]. Cet instant met en évidence l'indifférenciation entre le politique

---

Annuaire Français des Relations internationales, Vol. X, 2009.

[15] Thierry M., «Monarchie de Dante: de l'idée médiévale d'empire à la citoyenneté universelle» in Thierry Menessier (dir.), *L'idée d'empire dans la pensée politique, historique, juridique et philosophique*, Paris, L'Harmattan, 2006, P. 81-96.

[16] Schilling H., «la confessionnalisation et le système international» in Lucien Bely (dir.), *L'Europe des traités de Westphalie: Esprit de la diplomatie et diplomatie de l'esprit*, Paris, 2000, pp.411-428.

[17] La «défenestration de Prague» est la conséquence des antagonismes religieux, économiques et politiques qui traversent l'Europe centrale au début du 17è siècle. Incarnée par un acte de violence commis au Château de Prague où Martinic et Slawata sont précipités d'une fenêtre par les protestants des états de Bohème suite à la violation par l'empereur Mathias

et le religieux. Dans une Europe qui a longtemps caressé le rêve d'une unité politique inspirée de la *pax romana*. La maison d'Autriche ayant fait prospérer les ambitions des Habsbourg qui visaient une monarchie universelle fondée sur l'unité de la chrétienté[18].

Cet ambitieux projet qui aurait fait obstruction à l'émergence de multiples Etats fragmentés sous l'effet, à la fois, de l'émergence des maisons souveraines précurseurs des grands Etats européens, et de la rupture religieuse de 1517 incarnée par la réforme. Ainsi, d'une conception des relations internationales très marquée par le rêve impérial, l'on passe à un dualisme confessionnel caractéristique des rapports internationaux grevés d'une conflictualité épique. La guerre de trente ans sera donc une guerre confessionnelle juxtaposant une Europe catholique et une Europe protestante.

Schilling considère que de 1550 à 1650, cette «confessionnalisation» a fortement marqué les relations internationales, précédée par le facteur dynastique avant 1550 et suivie de la raison d'Etat au 17 siècle[19]. L'ordre des «maisons souveraines» n'a donc pas exclu l'ordre du religieux. Bien plus, ont-ils, par une commune congruence, renforcé le «tournant westphalien»: aiguillon politique et embrayeur idéologique, la «mobilisation des âmes conduit à celle des politiques», affirme Lucien Bely[20]. La règle *cujus regio, ejus religio* va renforcer cette consubstantialité bien qu'elle ait été l'un des ferments de la conflictualité entre les Habsbourg d'Espagne et du saint Empire (catholiques), et les princes des Etats allemands du saint Empire (protestants). Une véritable guerre civile européenne qui a été pourtant une «guerre allemande»[21]: parce que incarnant le Saint-empire et la bipolarisation religieuse. L'Allemagne a été l'épicentre de l'affrontement entre protestants et catholiques. Les auteurs comme Krummenacher ajoutent à ce clivage saillant, d'autres facteurs qui y trouvent leur exutoire notamment: les tentations hégémoniques et indépendantistes, les rivalités commerciales, les ambitions personnelles et les jalousies familiales[22].

---

des droits religieux concédés par la lettre de Majesté.

[18] C'est surtout sous Charles Quint que cette ambition devient universelle: voir Jean Bérenger, La monarchie universelle de Charles Quint in Georges Livet et Roland Mousnier (dir.), *Histoire générale de l'Europe* (12), Paris, PUF, 1980, pp.271 à 300

[19] «La confessionnalisation et le système international» in Lucien Bely, (dir), op.cit., P.416.

[20] Bely L., op.cit., P5

[21] Gantet C., «le tournant westphalien: Anatomie d'une construction historiographique», *Critique internationale*, vol.9, n°1, 2000, pp 52-58.

Au total, ce qui préfigure les traités de Westphalie, c'est la modification substantielle de l'équilibre des forces politiques en Europe. Si la France, la Suède, les provinces réunies et la Suisse sortent renforcées, l'empire quant à lui est éclaté et donne lieu à la multiplication d'Etats indépendants. De même que l'Espagne minée par les graves conflits de succession est presque décadente. Et comme l'émergence de l'Etat et son raffermissement se consolident dans la capture du «monopole de la contrainte légitime», l'on va assister à la constitution des véritables armées de métier[23].

Westphalie s'ouvre donc sur une Europe opérant «par et dans la pluralité des Etats»[24], la «raison d'Etat» se substituant à un «Empire européen des derniers jours»[25]. Les entités douées de souveraineté seront théorisées par Jean Bodin et Thomas Hobbes et actées par les traités de Westphalie.

2 - LES SUPPORTS THÉORIQUES ET JURIDIQUES DE LA PUISSANCE DE L'ETAT WESTPHALIEN

L'ordre westphalien tient à une configuration de la scène internationale dominée par les Etats souverains. Il met en place un monde des Etats largement tributaire des théories de Jean Bodin et de Thomas Hobbes. Vont être posées les bases du droit international moderne: «l'Etat en la personne du monarque, est suprême à l'intérieur de ses territoires, indépendants de toute autre autorité, et légalement égal aux autres Etats»[26]. Ainsi, le modèle politique qui instaure l'ordre westphalien se trouve au fondement de l'institution étatique que des nouvelles relations internationales du contexte Européen vont entériner. L'ordre de Westphalie est réellement un ordre continental qui a élargi son spectre à toute la planète. Il est supposé selon les Parties contractuelles de 1648, durable et régulé par des normes juridiques intangibles. Au surplus, il consacre, un nouvel équilibre géopolitique très structuré par la célébration de la théorie réaliste dans les rapports internationaux.

---

[22] Krumenacker Y., *La guerre de 30 ans*, Paris, Ellipses, 2008, pp 5-7.
[23] Bogdan H., *La guerre de trente ans*, Paris, éd. Perrin, 1999.
[24] Krumenacker Y., op. cit., p.152.
[25] Foucault M., *Sécurité, territoire et population*, cours au collège de France 1977-1978 Gallimard, Hautes Etudes, Paris, 2004, pp.131 et suiv.
[26] Bodin J., *Les six livres de la république*, Paris, Arthème Fayard, 1986.

Il n'est pas superflu de rappeler que l'ordre de Westphalie repose sur deux traités séparés fortement structurés par les clivages religieux - précaution diplomatique sans doute -pour éviter la résurgence d'un conflit religieux qui a traversé la guerre de trente ans depuis la «défenestration» de Prague[27]. Même si les traités n'ont pas clôturé la propension conflictogène des Etats dans les relations internationales[28], ils ont, en revanche, inspiré l'édiction d'un corpus des règles intangibles qui a assuré la régulation des rapports internationaux.

A - LA CONSTRUCTION JURIDIQUE DE LA PUISSANCE DE L'ETAT WESTPHALIEN

Cette construction repose sur le principe de souveraineté, «pouvoir ultime et perpétuel», et sur ses succédanés indispensables: les principes de territorialité et d'égalité.

- PRINCIPE DE SOUVERAINETÉ ET PRODUCTION D'UN ETAT DÉMIURGE

Avec Jean Bodin, nait ce concept toujours controversé dans l'histoire de l'humanité[29] qui git des entrailles des traités de Westphalie et élève l'Etat au pinacle de souverain unique et perpétuel. Constitue une république, selon Jean Bodin, toute cité capable d'assumer cette unicité et cette perpétuité en ne dépendant d'aucune autre entité souveraine. Il ne laïcise pourtant pas complètement l'Etat dans la mesure où la souveraineté demeure sous escarcelle divine. En effet, l'homme était la représentation miniaturisée de Dieu: le contredire constituerait une énorme transgression sacrilège. La souveraineté de Bodin joint une conception abrupte voisine d'une certaine

[27] Cet événement est sans doute le point de départ d'une «confessionnalisaion» des relations internationales. Puisque l'Etat qui en a résulté ne sera pas totalement expurgé de la gangue religieuse. Les trois traités signés sont au nombre de trois: La paix de Munster entre l'empire espagnol et les provinces unies, le traité de Munster entre la France et le Saint empire romain germanique, et leurs alliés respectifs, Le traité d'Osnabrück entre l'empereur du saint empire germanique et l'empire suédois.

[28] La France a malgré tout continué la guerre contre l'Espagne.

[29] Bodin (Jean), *Les six livres de la république*, op.cit., les critiques de Bodin sont consignées dans l'article de J.L Holzgrefe: «The origins of Modern International Relations theory», *Review of international studies*, 05 janvier 1989, pp 11-26

imprudence, et l'usage pratique du concept s'ouvre sur un totalitarisme[30]. Elle marque sans doute le contexte d'une France déchirée et d'un souverain incapable d'assurer l'unicité et la perpétuité de la souveraineté.

Les critiques de Bodin ne récusent pas le concept: il y a plutôt une reprise réchauffée de la notion qui charrie de fécondes intuitions renvoyant à une désacralisation de l'idée de souveraineté[31]. En regard, Grotius situe les actes de l'Etat en contrebas du droit naturel et du droit divin. L'Etat ne serait donc plus souverain dans l'absolu. Cette hiérarchie permet de tenir la souveraineté de l'Etat en lisière par un droit qui lui est supérieur. Cette idée est prémonitoire du droit international édicté contractuellement par les Etats. Le droit des gens qui constitue le rudiment du droit international contemporain participe alors de cette démarche limitative de la souveraineté de l'Etat par des obligations librement contractées qui lui sont opposables. Nous sommes là au cœur de la complexité de la notion: le droit des gens ne préempte pas la souveraineté des Etats, il procède à son exercice. Qu'elle loge dans le droit divin, le doit naturel ou dans le contrat (comme nous le propose Thomas Hobbes)[32], la souveraineté dans le contexte westphalien et post-westphalien a pour épicentre l'Etat, point d'irradiation et d'impulsion politiques.

«Invention complexe», tributaire d'une construction sociale, la souveraineté est d'ordinaire grevée d'élasticité. Sa compréhension pratique ne peut tenir qu'à un équilibre d'échassier imbriquant modérément la souveraineté et le religieux. C'est pourquoi, elle s'analyse en un équilibre qui échappe à la pesanteur des extrêmes:»un peu de souveraineté permet de construire les Etats contre la guerre civile: trop de souveraineté les conduit à s'entredéchirer. Un peu de religion limite l'arbitraire du prince:

---

[30] Badie (Bertand) , *Un monde sans souveraineté: les Etats entre ruse et responsabilité*, Paris, Fayard, 1999, p. 23

[31] Il s'agit de Grotius (Hugo), Droit de la guerre et de la paix, Centre de philosophie politique, Caen, 1984: voir également Smouts (Marie Claude), «Du côté de chez Grotius: l'individu et les relations internationales chez un ante-moderne»: in Bertrand Badie et Alain Pellet (dir.), *Les relations internationales à l'épreuve de la science politique*, Paris, Economica, 1993, pp. 383-395

[32] Hobbes (Thomas), *Léviathan ou Matière, forme et puissance de l'Etat chrétien et civil*, Londres, 1651: éd Gallimard, 2000: voir également dans une perspective théorique: *Eléments du droit naturel et politique*, Paris, Vrin, 2010. La thèse de Hobbes est une réévaluation du discours souverainiste qui tranche avec la perspective éthique et jusnaturaliste de Hugot de Groots.

trop de religion conduit à la dictature du synode»[33]. Précieuse invention de Westphalie, la souveraineté n'accroit sa capacité actancielle qu'en s'adjuvant les principes d'égalité et de territorialité.

- L'ORDRE WESTPHALIEN: UNE JUXTAPOSITION D'ETATS ÉGAUX, ET DE TERRITORIALITÉS

Si la paix de Westphalie consignée dans les traités est considérée comme le document diplomatique le plus évoqué dans l'histoire européenne, c'est en raison d'une systématisation complète des principes régulateurs de l'Etat et de ses rapports internationaux: les principes de souveraineté, d'égalité et de territorialité ont donc partie liée. Ciapin les met en synergie pour décrire une situation où, «les Etats se reconnaissent mutuellement comme seuls interlocuteurs légitimes et définissent les traités comme outils mutuels reconnaissant les souverainetés et les tracés frontaliers des parties en fixant les lignes de front en frontières[34].

Le principe de territorialité renvoie à la délimitation des ensembles géographiques par des territoires sur lesquels s'exercent la souveraineté interne des Etats et leur contrôle: ce principe proscrit l'ingérence et donne à l'Etat-nation la légitimité exclusive de juridiction sur son territoire. La notion de territoire est nécessairement associée à celle de frontières[35]. Dans le système westphalien, la construction territoriale a constitué la base essentielle de l'institutionnalisation des rapports entre Etats car, «il n y a pas depuis 1648 d'ordre international, de système international qui ne reposent sur cette conception, d'où cette crise que nous vivons maintenant», écrit Betrand Badie[36]. Et puisque la science politique aborde la question de territoire par son usage, Max Weber le lie fondamentalement à son usage politique et en fait un espace d'exercice continu de la contrainte légitime[37].

---

[33] Badie (Bertrand), *Un monde sans souveraineté*, op.cit., p.24.

[34] Ciapin (Etienne), *Frontières, et populations: territoires mobiles, voisinage européen*, thèse de sociologie, université de Grenoble, Alpes, 2010, p.81

[35] Georges (Pierre), *Dictionnaire de la géographie*, 1974.

[36] Badie (Bertrand), in «territoires, lien ou frontières», Paris, 2-4 octobre 1995

[37] Weber (Max), *Le savant et la politique*, trad. de l'All. Par Catherine Colliot-Thélène, Paris, La Découverte, 2003: pour mieux expliciter la pensée de Weber, lire C-Colliot Thélène, «La fin du monopole de la violence légitime ?», *Revue d'études comparatives Est-Ouest*, vol. 34, n°1, pp.5-31.

L'approche fusionnelle de politique et du territoire supplante donc les divisions ethniques, c'est pourquoi conçu dans cette perspective, l'ordre westphalien a révoqué les particularismes, désormais noyés dans l'Etat-nation où le territoire devient le principe actif de l'ordre politique. La configuration et le bornage de l'espace territorial «deviennent le principe structurant de la communauté politique et mode discriminant de contrôler une population, de lui imposer une autorité, d'affecter et d'influencer son comportement»[38].

L'ordre n'admet *in fine* aucun désordre, c'est une juxtaposition de souverainetés, de territorialités, mais aussi d'égalité. Le principe d'égalité entre Etats constitue l'un des principes fondateurs de l'ordre westphalien: héritage fondamental de l'ordre westphalien, il était étranger au système international, incarné par l'Empire du milieu autour duquel gravitaient le Japon, la Corée et l'Annam. Contrairement au paradigme westphalien, l'Asie dans son ensemble avait une conception hiérarchisée des rapports entre Etats. Les relations internationales étaient des relations «tributaires»: l' «Empire du milieu» exerçant un fort tropisme sur les Etats tributaires par le truchement de l'institutionnalisation d'une ingérence chinoise dans la vie socio-économique et politique[39].

Le principe d'égalité est synonyme de non-ingérence et considère que le droit international a pour unique source les traités négociés et signés d'égales parties entre les Etats. Il induit l'équilibre de puissance où les Etats pèseraient d'un même poids sur la scène internationale. Il s'agit sur le plan juridique de l'égalité souveraine entre Etats: l'inter - étatisme vise une «horizontalisation» des rapports entre les Etats en passant par les pertes et profits les inégalités réelles qui les traversent[40]. Consacré par la Charte des Nations Unies[41], le principe d'égalité entre les Etats renvoie à la souveraineté externe. De l'ordre westphalien découle également l'idée que les Etats ne sont soumis à aucune instance supérieure: ils ne sont

[38] Sack (Robert), *Human territoriality: its theory and history*, Cambridge, Cambridge university press, 1986, pp.17-19.
[39] Vinay-Postel K., «la frontière ou l'invention des relations internationales», *CERISCOPE frontières*, 2011.
[40] Godefray N. -Marfin Sermang ngakisso, «L'égalité souveraine des Etats aujourd'hui ?, *Journal de la recherche scientifique de l'université de Lomé*, vol 21, n° 3, 2019.
[41] Article 2 Paragraphe 1

minimalement soumis qu'aux seuls droits auxquels ils ont consentis. Etant juridiquement égaux, ils jouissent des droits inhérents à leur pleine souveraineté, ils ont le droit de choisir et de développer leur système politique, social, économique et culturel[42]. Ordre de souveraineté d'égalités, de territorialités, l'ordre westphalien est un ordre de puissance que consacre la théorie réaliste dans les relations internationales.

B- ORDRE WESTPHALIEN: FONTS BAPTISMAUX DE LA CÉLÉBRATION DE LA THÉORIE RÉALISTE

L'idée de la superpuissance découlant des considérations historiques de la nomenclature internationale est tributaire de l'ordre westphalien. C'est un ordre subtil d'accommodation à la guerre puisque les conflits entre Etats-nations devaient, auparavant, faire l'objet d'une déclaration préalable. Les Traités de Westphalie ne consacrent donc pas une clôture de la belligérance, mais une règlementation flexible de son occurrence. La notion de «juste cause de la guerre» va animer le débat philosophique depuis Grotuis[43] et s'inspirera pour l'essentiel des théories morales et théologiques. En tout état de cause les Etats se «considèrent comme légitimes dans la paix comme dans la guerre»[44], la théorie réaliste tire son assise de cette légitimation feinte de la guerre.

L'on n'imagine pas apparaître dans ce contexte ce que Nye Joseph[45] appelle le «troisième échiquier» qui consacrerait les acteurs non étatiques et les forces transnationales avec une dispersion de pouvoir échappant au contrôle des Etats. La vie internationale de l'ordre westphalien s'inscrit dans le courant du réalisme classique qui, surestimant le rôle de l'Etat, a propagé une vision paranoïaque des relations internationales. Hans Morgenthau, Edward Hallett Car et Raymond Aron ont, malgré quelques

[42] Résolution 2625 (XXV) du 24 octobre 1970 sur la déclaration relative aux principes touchant les relations amicales et la coopération entre Etats conformément à la Charte des Nations Unies.

[43] Sur la contribution de Grotius à cette notion, voir le livre de Peter Haggenmacher, Grotuis et la guerre juste, Paris, PUF 1984.

[44] Brunsteller D. et Holeindre J. V., «La guerre juste au prisme de la théorie politique», *Raisons politiques*, vol.1, n°45, 2012, pp. 5-18.

[45] Nye J., The Paradox of the American Power: Why the world only super power can't go it alone, Oxford, University press, 2000, p. 35

nuances et variations, eu la même focale analytique: l'anarchie dans les relations internationales structurée par les Etats-nations, acteurs principaux et rationnels qui cherchent à maximiser leur «intérêt national»[46]. La théorie réaliste classique culmine sur l'équilibre des puissances comme antidote pour une stabilité internationale toujours précaire.

Evitons, toutefois, de céder à un anachronisme: il serait caricatural de rattacher historiquement l'émergence de la théorie réaliste à l'ordre westphalien alors qu'elle nait dans un contexte d'apparition de nouveaux Etats hors du contexte européen, des rapports de forces et d'équilibre de tension. Cet Etat demeure un ordre du vieux continent, très marqué par la théocratie.[47] La guerre du Péloponnèse entre Spartes et Athènes qui a inspiré Thucydide est, bien de loin antérieure, à l'ordre de Westphalie. Westphalie est donc un point nodal de la compréhension historique de l'érection de l'Etat comme acteur unique des relations internationales. C'est un marqueur important de l'expression de la puissance, qui va déteindre considérablement sur les représentations que les acteurs internationaux se feront de l'Etat sur la scène internationale. Parler de «tournant westphalien» comme le propose Claire Gaulet revêt toute sa signification paradigmatique: car de toutes les guerres, celle de 30 ans a été révélatrice de la question de puissance dans les relations internationales. La «fin des territoires … dans un monde sans souveraineté» n'incline pas à l'imagination d'un substitut fonctionnel à l'Etat, qui demeure *mutadis mutandi* l'instance prioritaire et légitime de la projection à l'international.

Naturellement, la théorie, réaliste en raison de la métamorphose de la scène internationale, devait administrer progressivement la preuve de son opérationnalité limitée. D'ailleurs, les variantes théoriques du réalisme perturbent déjà sa cohérence générale: la perspective classique qu'incarne principalement Hans Morgenthau se double de trois approches pas toujours convergentes dans leur dispositif théorique: le réalisme structurel de

[46] Voir Morgenthau H., *Politics among Nations: The Struggle for power and peace*, New York, Knopf; 1948; Aron (Raymond), *Paix et guerre entre les nations*, Paris, Calmann Levy, 1962.

[47] Très inspirée de la lecture que fait Thucydide de la guerre du Péloponnèse et des philosophes comme Thomas Hobbes, elle n'a pas manqué d'être influencée par le théologien américain Reinho Niehuher qui part du postulat religieux pour appréhender les relations internationales par le courant du réalisme chrétien (voir *Moral man and immoral society: a study of ethics and politics*, Westminster, John Knox Press, 2002)

Kenneth Waltz contraste quelque peu avec le réalisme néoclassique de Gideon Rose, et bien plus avec la synthèse néoréaliste et néolibérale de Robert Keohane[48]. Cette dispersion théorique ne présage- t- elle pas d'une fragilité explicative révélée par les «turbulences» mondiales ? En tout cas, le monde des Etats issus de Westphalie est désormais challengé par le «monde multi centré». D'où des linéaments d'une émasculation du corps hermétique de l'Etat.

B- LES LINEAMENTS D'UNE EMASCULATION DU CORPS HERMETIQUE DE L'ETAT

La mondialisation actuelle qui trouve ses origines dans la réalité historique du 19e siècle jusqu'à la Première Guerre Mondiale[49], était de nature à rogner les souverainetés des Etats, à rendre labile la territorialité, et impertinent le principe d'égalité entre Etats. Ses principes sont, aujourd'hui, en question: et plus spécialement le territoire dont la surestimation de l'importance politique relève d'une culture occidentale très liée à la construction de l'Etat dès la fin du moyen âge. Bertrand Badie en déduit que son extension à d'autres cultures ne pouvait être que porteuse d'ambiguïtés[50]. La «fin des territoires» est aussi l'expression métaphorique d'une labilité des frontières.

1 - UNE TERRITORIALITÉ LABILE

La question territoriale suscite aujourd'hui une réflexion sur son sort

[48] L'on peut sérier le réalisme en quatre grands courants: le courant classique de H. Morgenthau, R. Aron, E. H. Carr (en opposition à la pensée libérale qui selon eux n'a pas empêché le déclanchement de 2è Guerre mondiale, l'Etat souverain est désormais au cœur des relations internationales, sa politique étrangère doit être pensée distinctement, et la défense des intérêts nationaux définie en termes de puissance devient la clé de compréhension de l'action de l'Etat sur la scène internationale, l'équilibre des puissance devient la solution à l'éventualité d'une guerre) , le courant néoréaliste ou structurel de K. Waltz (cette théorie considère que la première préoccupation des Etats c'est leur sécurité et non la quête de puissance, c'est une approche structuraliste dans la mesure où le seul déterminant des relations internationales c'est le système international), le réalisme synthétique qui combine réalisme et libéralisme avec R. Keohane qui a une conception systémique qui postule que la posture de l'Etat à l'international est dictée par les pressions exercées sur lui par une concurrence internationale qui structure ses choix, enfin le réalisme néoclassique qui introduit les variables systémiques intermédiaires, cognitives, et nationales dans le comportement de l'Etat dans les RI).

[49] Badie B., Smouts (Marie-claude), *Le retournement du monde: sociologie de la scène internationale*, Presses de science Po et Dalloz, Paris, 1999 (3e Edition).

[50] Badie B., *Un monde sans souveraineté*, op.cit.,

dans un contexte d'émasculation des fondements existentiels classiques de l'Etat. La confusion entre la communauté politique et la communauté territoriale est un fait auquel les irruptions des systèmes d'allégeances concurrentiels dérogent. La thèse de l'émergence des «nouveaux territoires» prend du corps et annonce les linéaments d'une émasculation de l'ordre hermétique westphalien. Le recours à l'Etat devient une alternative aléatoire challengée par les nouvelles communautés de responsabilité. L'on assiste à un phénomène de «territorialité défaillante» ou «d'espace irréel»[51]. La circulation des idées, la proximité quasiment intensive des hommes, l'émergence des acteurs transnationaux (ATN) font que la fonction politique de l'Etat décline vertigineusement.

L'ordre westphalien et post-westphalien où le territoire a été la seule variable de codification des relations internationales se mue insensiblement en un lieu de «turbulence». C'est dans ces flux transnationaux que se meut l'essentiel de la vie sociale, économique, culturelle et où se construisent des nouveaux imaginaires territoriaux transgressifs: le paradoxe est que l'on ne comprend pas que le territoire qui dans la définition de Max Weber, constitue un trait saillant de la modernité politique[52], se trouve aujourd'hui challengé par les agents de la modernité. La clé de l'énigme réside sans doute dans le potentiel d'investissement symbolique des acteurs sociaux qui construisent autour du principe de territorialité un sens novateur.

L'on ne peut parler de territoire de l'Etat sans évoquer la problématique la plus débattue de la dernière décennie: celle de la «fin des territoires» qui a bénéficié d'une très large audience. Celle-ci tient aux bouleversements spectaculaires qui ont marqué la scène internationale. Sa légitimité est en partie liée avec une lecture «par le fil du social»[53]. S'il est vrai comme l'affirme Badie que «la révolution des communications a ouvert de nouvelles routes mondiales qui n'ont plus de base étatique, l'internet, le téléphone, le satellite ont libéré l'individu de toute sectorisation géographique[54]: l'ordre westphalien et post-westphalien charrie les effets

[51] Igué J O, *Le territoire et l'Etat en Afrique: les dimensions spatiales du développement*, Paris, Karthala, 1995, pp. 8-19
[52] Weber M., *Le savant et le politique*, op.cit.
[53] Badie B., «Le monde par le fil du social» in Fondation Gabriele Peri, La pensée, N° 387, 2016/3, pp. 21-27: il soutient en effet que le premier modèle d'ordre mondial «se faisait politique et tenait, par définition le social à l'écart» (p.1)

d'un «habitus», générateur et régénérateur. Plus précisément, l'Etat westphalien a été un «cadre d'expérience» modélisé par «le pouvoir transnational» des nouveaux acteurs transnationaux: pour pasticher Erving Goffman, l'Etat westphalien est un «cadre primaire qui se transforme en une autre activité qui prend le cadre primaire pour modèle, mais que les participants considèrent comme sensiblement différent»[55].

En tout état de cause, il y a une labilité des frontières que confortent une souveraineté et une égalité entre Etats, sérieusement rognée.

Des souverainetés rognées

L'élargissement de la scène internationale consécutif à l'émergence des nouveaux Etats a créé un monde de «souveraineté» et d'égalité, bien que très marqué par l'hégémonie occidentale qui consacre une hiérarchie de puissances. Les principes d'égalité et de souveraineté qui n'ont de véritable signification que dans le contexte européen de l'équilibre entre les Etats apparus sous les traités de Westphalie. Les philosophes qui ont inventé le concept de souveraineté l'ont surchargé de complexité au point d'en avoir une appréhension sublimement fictionnelle. Cette mystérieuse idée de souveraineté, «puissance ultime et perpétuelle» se confond selon Jean Bodin à la république. Les nuances philosophiques de Grotius et de Locke[56] annonçaient les difficultés d'une circonscription conceptuelle, auxquelles allait s'ajouter la fragilité d'une notion épurée par les mutations contemporaines de la société internationale. La guerre de trente ans était déjà le terrain empirique de la construction théorique d'une souveraineté «réaliste» où le droit international ne pouvait plus s'appréhender comme une réalité tributaire de l'unique volonté des Etats. Grotius «campait déjà parfaitement notre sujet» écrit Bertrand Badie, puisque l'on «entrevoit déjà les problématiques de notre époque: marché international, guerres injustes, la sanction de ceux qui sont coupables, la protection des biens communs, etc…»[57]

C'est cette vision du monde, encore en linéament, qui va annoncer

[54] Badie B., «Nous sommes plus seuls au monde: nouveaux regards sur l'ordre international», Paris, La Découverte, 2016

[55] Goffman E., *Les cadres de l'expérience*, Paris, Minuit, 1991, p.52.

[56] Grotius va s'inscrire en contrepoint de cette conception «totalitaire» en lui opposant le droit naturel et le droit divin, considérés comme supérieurs aux actes de l'Etat. Pour l'auteur, Des traités du gouvernement civil, l'Etat souverain ne constitue pas une puissance ultime, mais le cadre de réalisation d'un mandat que lui confie le peuple conformément au droit naturel.

[57] Badie B., *Un monde sans souveraineté: les Etats entre ruse et responsabilité*, Paris, Fayard, 1999, p24.

l'ivresse de la métamorphose qui s'est emparée de la scène internationale. Depuis 1990, toute une littérature déchainée décrète l'obsolescence de la politique étrangère[58]. La thèse marxiste du dépérissement de l'Etat est réchauffée à l'aune de l'activisme des acteurs transnationaux charriant les organisations non-gouvernementales, firmes multinationales, terroristes, migrants, trafiquants, des drogués, mouvements terroristes, etc.

Sans céder à cet affolement pessimiste sur le sort funeste de l'Etat, l'on note, au travers de l'empirisme, des faits une foire d'empoigne entre le «monde des Etats» et le «monde multi centré». Est privilégié dans l'approche scalaire de Joseph Nye, le «troisième échiquier» qui consacre une dispersion de la puissance exempte de tout contrôle étatique. En tout état de cause, l'Etat projette l'image d'une souveraineté rognée par les acteurs transnationaux et d'une territorialité labile. Reste le principe d'égalité que la configuration de puissance ramène à une clause de style, voire à une pétition de principe. Dans la nomenclature de Nye, la puissance, mieux l'inégalité est consacrée dans le premier et le deuxième échiquier où l'on retrouve prioritairement les Etats-Unis, le Japon, l'Europe et la Chine. Consacré par les articles 1 et 2, paragraphe 1 de la Charte des Nations Unies comme fondement de la coopération entre Etats, le principe d'égalité apparait simplement comme un «acte de langage»[59] aux effets déclaratoires et «constatifs»: la hiérarchie des puissances mettant naturellement en cause l'égalité entre les Etats qui n'est, *in fine* qu'une égalité factice. En tout cas, l'Etat est «appelé Etat quand il est passif, et souverain quand il est actif» écrivait Jean Jacques Rousseau[60].

Il y a plus, les Organisations Internationales ont développé des compétences propres en marge de celle des Etats membres: pouvoirs supa-nationaux qui s'imposent dans le droit interne des pays membres: l'ONU, l'OMC, l'UE et même les ONG et les entreprises privées mondialisées

[58] Strobe T., «globalization and diplomacy: a practitioner's perspective», *Foreign policy*, hiver 1997; S. Strange,*The diffusion of power in world economy*, Cambridge university press, Cambridge, 1996; Thomas-Kapen, «Bringing transnational relations back», in Non-state actors, domestic structures and international institutions, Cambridge university press, Cambridge, 1995.

[59] Austin J. L., *Quand dire c'est faire*, Paris, Seuil, 1972: les actes de langage constatifs ne visent pas à modifier les représentations des choses et des buts: il s'agit tout simplement de dire quelque chose et non de dire quelque chose en faisant.

[60] Du contrat social, livre I, chapitre VI

s'emploient dans une forme d'ingérence subreptice qui n'a aucun mal à s'imposer aux Etats: il y a même un glissement sémantique, aujourd'hui vers l'immatérialité de la souveraineté. L'on parle ainsi de souveraineté numérique dont l'une des caractéristiques contemporaines est la tenue par plusieurs Etats des registres des métadonnées Doblin Core contrôlant des informations en sources ouvertes. La pratique du *social Bookmaking* de partage des signets n'a pas seulement le brillant de la libre communication, elle rogne insidieusement la souveraineté de l'Etat[61]. Il y a cependant dans ce domaine une situation de quasi-monopole technique et économique des multinationales américaines notamment dans la maitrise du système d'exploitation et du développement des applications numériques[62]: d'où l'inquiétude de certains Etats qui réclament leurs droits souverains sur la gestion du réseau et un traité international de partage des responsabilités.

Il y a une floraison des métalangages virtuels suite à l'Affaire Snowden (2014): «territoire numérique», «souveraineté» qui dans l'ordre westphalien pourraient être considérés comme une transgression sacrilège. Ils s'imposent pourtant dans le champ cognitifs et correspond selon Pierre Bellanger à la «maitrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques»[63]. D'ordinaire, la tendance aujourd'hui est celle du prolongement de la souveraineté de l'Etat dans l'espace numérique plutôt que d'imaginer de nouvelles formes de souveraineté ? Dans cette perspective, la souveraineté de l'Etat n'en prendrait pas un coup, puisque, la souveraineté numérique demeure celle des Etats qui prolongent leur pouvoir réglementaire général sur le cyberespace[64].

Somme toute, quel que soit l'orientation que l'on puisse donner au concept de souveraineté numérique, il demeure constant que l'Etat post-westphalien est aujourd'hui éprouvé par «la plus grande expérience d'anarchie de l'histoire»[65] qu'est internet. L'ordre westphalien ainsi

[61] Hammond T., Hannay T., Scott J., Social book marking tools (I): A general Review in D. Lib Magazine, 11, n° 4, 2005.
[62] L'ICANN (internet Corporation for Assigned Names and Numbers), société californienne qui constitue la racine stratégique de l'internet.
[63] Bellanger P., *La souveraineté numérique*, Paris, Stock, 2014.
[64] Turk P., «La souveraineté des Etats à l'épreuve d'internet», *Revue de droit public*, n°6, 2013.
[65] Schmidt E., Cohen J., *The new digital Age*, Knopf, 2013, (trad, A nous d'écrire l'avenir, Paris, Denoél, 2013, p.11.

fragilisé par une mondialisation disruptive qui a favorisé l'irruption des systèmes d'allégeances concurrentiels. Cet ordre n'est donc pas un mythe usé, tout au moins ne renouvelle-t-il pas profondément son fonctionnement ?

II - L'ORDRE WESTPHALIEN FRAGILISÉ PAR UNE MONDIALISATION DISRUPTIVE: LES NOUVELLES ALLÉGEANCES SOUS L'EFFET DE LA CIRCULATION DES IDÉES

La mondialisation est directement liée au processus de mutation qu'éprouve actuellement l'Etat. Puisqu'elle a été disruptive, et a permis «de faire émerger des visions nouvelles qui sont à l'origine des grandes innovations»[66]. Elle est bien plus une «destruction créative» à laquelle Joseph Schumpeter associe les nouveaux moyens de communication[67]. Elle porte en elle la puissance de la dynamique de changement à l'épreuve dans les relations internationales et l'essor des sociétés grâce aux nouvelles technologies.

Les nouvelles technologies facilitent la circulation des idées et le partage des convictions, et aménage les conditions d'une quasi-intensité de la proximité entre les hommes. La souveraineté des Etats est ballotée non seulement par l'interdépendance entre eux, la montée en puissance des organisations internationales, la mondialisation économique, le développement des échanges internationaux, mais surtout par l'irrésistible expansion du libéralisme numérique[68]. Les NTIC sont en effet une «structure des opportunités» d'actions aussi bien pour l'Etat que pour les acteurs transnationaux: ils s'en emparent pour la fabrication d'un sens novateur à travers une mise en récit qui légitime aux cotés de l'Etat des

[66] Ala philippe L., «La disruption: une méthode qui fait chemin, ou comment la rupture peut devenir une stratégie d'innovation, sur Lesechos.fr, 7 nov 2016, consulté le 04 avril 2012: voir également Jean Marie Dru, Disruption overturning conventions and skaking up the marketplace, John Wiley and sons, Aweek magazine series, 1996.
[67] Schumpeter J., *Capitalisme, socialisme et démocratisation du monde*, Paris, L'échappée, 2016, p. 24.
[68] Sadin E., la siliconisation du monde: l'irrésistible expansion du libéralisme numérique, Paris, L'échappée, 2016, P. 24

nouvelles allégeances. Des nouvelles compréhensions du monde se font jour grâce aux techniques: la forme la plus élaborée de cette mise en récit réside dans le «*Storytelling*»[69], cette accroche novatrice capable de créer un «monde de choses».

A - LA PROFUSION DES «STORYTELLING» DANS LA CONSTRUCTION ET LA LÉGITIMATION DES NOUVELLES ALLÉGEANCES

La cybernétique sustente les médias de masse et leur font acquérir une diffusion à grande échelle pour répondre à une demande d'information d'un public toujours plus vaste. Les médias sont des outils et le *storytelling* ce qu'en font les acteurs sociaux. Le *storytelling* est fort aise dans un contexte cybernétique qui signe l'avènement des médias alternatifs, permettant de lire les relations internationales autrement que par le fil du politique. Cette effrayante «machine à fabriquer les histoires et à formater les esprits» met en exergue l'importance de nouveaux usages du récit dans la communication. Il constitue «un nouvel ordre narratif», selon Salman Christian[70].

L'on peut donc saisir l'irruption des systèmes d'allégeances concurrentiels à travers la focale analytique de la légitimité et de la représentation comme nouvel enjeu de puissance.

1 - LE STORYTELLING ET LA CONSTRUCTION D'UN RÉGIME DE VÉRITÉ FACTICE

Toute réalité sociale, pour reprendre Peter Berger, est une construction[71]: lorsqu'elle s'inscrit dans une perspective concurrentielle, elle revêt un caractère idéologique renvoyant à une lutte d'imposition d'un régime de vérité. Deux constats peuvent être faits en guise d'hypothèses: *prima facie*, nous assistons à l'émergence d'un monde où les acteurs internationaux

[69] Salman C., *Storytelling, la machine à fabriquer des histoires et à formater les esprits*, Paris, La Découverte, 2007.
[70] Salman C., *Ces histoires qui nous gouvernent*, Paris, JC. Gawsewitch, 2012.
[71] Berger P., *La construction sociale de la réalité*, Paris, Méridiens Klincksiek, 1986.

rivalisent dans la «fabrication du consentement»[72], et où se profile une «ère post vérité» que charrie l'inflation du canular informatique (hoax). Ensuite, ce nouvel ordre narratif bute sur la floraison de contre narrations qui visent une remise en cause ou mieux une mise en débat du discours de la norme, ou se construit tout un répertoire d'actions stratégiques. Dans le storytelling, les «faits objectifs ont moins d'importance pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles»[73].

Deux exemples suffisent à simplifier l'accessibilité à ce concept dans l'entreprise de construction factice d'un régime de vérité: le président George Bush et la justification de son approche réaliste des relations internationales lors de la guerre du Golfe, et le discours islamiste salafiste diversement articulé par les composantes disparates de l'Etat islamique.

Le président George Bush use à profusion du storytelling dans ses prises de paroles post-onze septembre. Il s'abonne à toute une organisation rhétorique qui fixe sa base lexicale sur un vocabulaire schmittien, qui d'ordinaire pense le politique sous le prisme de l'ami/ l'ennemi. Il repose sur un «discours de constitution d'une histoire unique qui donne un sens à des éléments fragmentés et qui permet à celui qui l'utilise de légitimer des message ou des actions, de réaliser les intérêts personnels déterminés». George Bush joue sur la transmutation sémantique qui opère sur le mode des «actes de langage» perlocutoires, glissement et déplacement de sens qui construisent une cohérence discussive sur la lutte contre le terrorisme: ainsi la «guerre contre le terrorisme est une «guerre contre la terreur», mais surtout une «guerre pour la liberté».

Dans un discours de *graduation ceremony* à West Point en 2002, il annonce une rupture de paradigme: «de nouvelles menaces impliquent de nouvelles politiques, la dissuasion ne veut plus rien dire contre des réseaux terroristes invisibles, sans nation ni citoyens à défendre. L'endiguement n'est pas possible quand les dictateurs avec des armes de destruction massive peuvent fabriquer d'autres armes et les transmettre à leurs alliés terroristes… Nous devons attaquer l'ennemi et le mettre en déroute,

[72] Ghomsky N., *La fabrication du consentement: de la propagande médiatique en démocratie*, Paris, Agone, 2008.
[73] Dictionnaire d'Oxford, in la Presse.ca, 16 novembre 2016.

confronter les pires menaces avant qu'elles n'émergent». La construction de l'ennemi passe aussi par l'exacerbation du danger qui pointe à l'horizon:»lorsqu'il se produit une prolifération d'armes chimiques, biologiques et nucléaires, et qu'existe la technologie pour la fabrication des missiles balistiques, même les Etats faibles et les petits groupes peuvent accumuler une puissance catastrophique leur permettant de frapper les grandes Nations. Nous avons surpris nos ennemis en train de fabriquer les armes terribles».

L'ennemi est tout trouvé comme l'avait fait avant l'intervention militaire, le Général Collins Powell le 5 février 2003, une fiole à la main contenant de l'anthrax: «il n y a aucun doute que Saddam Hussein a des armes biologiques et la capacité d'en produire rapidement davantage…et il a la capacité de repandre ces poisons et maladies mortels de façon à provoquer des morts et destructions massives».

Cette lutte antiterroriste que sous-tend une mobilisation hardie contre la prolifération nucléaire, va se muer sensiblement en fabrique idéologique emportant le combat contre les dictatures, lutte pour la liberté, la démocratie et la paix. Le triomphe du modèle américain tient tout de même par une sorte de propagande par les rêves[74]. Le Président Bush a la claire conscience qu'on ne doit sa légitimité qu'à son détriment: d'où un art tout particulier de nommer les choses par l'usage «des mots magiques»[75], qu'il s'emploie à n'en donner aucune signification précise. Le «combat contre les dictatures» que Patrick Charaudeau considère comme un masque du pouvoir[76], réalise son chant de cygne dans une opération rhétorique de projection et de célébration du modèle américain de démocratie: «l'histoire de l'Amérique est l'histoire de la liberté en marche: un cercle toujours plus large qui s'étend constamment pour aller plus loin et inclure davantage l'engagement fondateur de notre nation demeure notre engagement le plus profond: dans le monde et chez nous, nous étendons les frontières de la liberté[77]. L'invasion américaine de l'Irak a donc une fonction émancipatrice

[74] Masson A., *La propagande par les rêves ou le triomphe du modèle américain*, Paris, Autrement, 1991.
[75] Augé E. F., *Petit traité de Propagande à l'usage de ceux qui la subissent*, Bruxelles, De Boeck, 2007, P.121-122.
[76] Charaudeau P., *Le discours politique: Les masques du pouvoir*, Paris, Lambert-Lucas, 2014.
[77] George Bush à la convention républicaine de New-York, le 2 septembre 2004.

qui permet au président Bush de mettre en valeur l'éthos à l'intérieur du récit, car contre la terreur, la démocratie est la seule antidote. Ce récit lui a permis de légitimer un agenda politique et militaire, par une fixation de la force pour maximiser les gains politiques en axant sa base lexicale sur un vocabulaire puisant dans le registre néoconservateur et réaliste.

Cette construction imaginaire du réel se retrouve dans le discours opposé des islamistes qui construisent en contrepoint une *weltanschauung* hostile à l'occident. Si nous nous intéressons singulièrement au Boko Haram, un des mouvements islamistes salafistes les plus dévastateurs, le corpus de leurs prêches et de leurs discours permettent de cerner l'idiosyncrasie propagandiste de ce mouvement.

Boko Haram n'a certainement pas les outils de communication que Daech, qui a une vidéothèque et une médiathèque jihadistes fournies, et qui associe propagande globale de masse sur le web et approche individuelle sur les réseaux sociaux. En ce sens, Pierre Conesa, François Bernard, Hyygle et Margaux Chouraqui affirment que Daech «dispose d'une organisation professionnalisée qui crée des produits adaptés aux groupes cibles: portraits, jeux de guerre, films publicitaires, reportages, clips musicaux, vidéos, post-attentats»[78].

Le système médiatique de Daech est gigantesque et est composé des médias traditionnels et une vingtaine de revues en arabe, français, russe, allemand, anglais et turque dans un souci d'élargissement du spectre de l'audimat. La manipulation experte des images d'horreur s'inspire moins de l'iconographie Islamo-arabe que des codes hollywoodiens avec un traitement très sophistiqué des images en termes de cadrage, de prise de vue et des systèmes de tournage à l'aide des grues pour travelling, des caméras haute définition, une musique assortie d'effets spéciaux et parfois l'usage des drones. L'Etat islamique s'est construit une indépendance médiatique par un usage stratégique de toutes les plates-formes offertes par les services de microblogging: ainsi le branding permet un «marquage au fer» de l'image de l'Etat Islamique à travers Twitter, Facebook, Istagram,

[78] La propagande francophone de Daech: la mythologie du combattant heureux, Fondation Maison des sciences de l'homme, pp. 28-35.

Télécom, You Tube et les outils du web 2.0. Les techniciens parlent d'une habilité toute particulière de l'Etat Islamique à faire usage d'un dispositif de référencement sur web associant Hastag et des comptes en arborescence. Dans l'application des messages instantanés Télégram où l'application cliente est gratuite, les «brigades médiatiques» du Daech ont la possibilité de migrer d'un compte à l'autre en réponse à la censure.

La typologie filmique de Daech privilégie les portraits projetant sur le devant de la scène les prouesses du prosélytisme islamiste, ainsi que les jeux de guerre assortis d'écopées et des décapitations avec une incarnation du héros des jeux vidéo «*Counter strike*»: il y a comme un «Daechwood» qui magnifie «une exaltation purement formelle de l'acte violent»[79]: toute une esthétique de l'horreur qu'accompagnent des épopées eschatologiques. Le long métrage sorti en 2014 «*The flames of war*», est une narration de la conquête de la Syrie et de l'Irak par les élus de Dieu, «*choosen by Allah*, *the few* of few, *from all corners of the world*». Un univers du «*Mujaweets*» se construit dans la fiction, qui tourne en dérision l'opulence occidentale en proposant une vie simplifiée dans les spots publicitaires: la technique des plans esthétisants est mise à contribution pour valoriser une vie modeste et paradisiaque en contrepoint de l'arrogance mécréante affichée par les Occidentaux.

Les rêveries islamistes de Daech font résolument dans la pédagogie fictionnelle comparative afin de tirer le parallèle avec des grandes Nations occidentales dont le territoire est aussi grand que ceux de la Grande Bretagne et de la Belgique. Est inscrit sur le fronton du spot publicitaire «*No respite*» et sous enseignes lumineuses l'apothéose mémorable qui tire sa légitimité historique de l'acte fondateur de 1435: «*this is the kalifah in all its glory. Remaining and expanding. It was established in the year 1435, its territory is already the size of GB*, eigth *times the size of Belgium*». Et surabondamment, les vidéos, posts, attentats servent également à magnifier le sermon d'allégeance du *De cujus*[80].

[79] Nossiter J. in Le Monde, 19 décembre 2015.

[80] La diffusion de ces vidéos a eu lieu respectivement le 15 Janvier 2015, en novembre 2015, mars 2016 à Bruxelles et à Paris et en été 2016 à Orlando, Nice, Saint-Etienne du Rouvray.

Ces outils médiatiques vont permettre à Daech qui est un mouvement salafiste jihadiste de projeter un Etat musulman s'étendant de l'Afrique du nord à l'Asie Centrale[81]. La grande dissidence de l'Etat Islamique, c'est l'émergence réelle ou fictive d'un Etat qui défie les frontières de l'ordre westphalien, un ordre très marqué de l'empreinte occidentale. La bataille médiatique sur fond de storytelling pose néanmoins un problème de fond: celui de la souveraineté numérique très sérieusement challengée par une activité effrénée et résiliente des Hackers qui fouinent jusqu'aux domaines les plus réservés de l'Etat.

2 - LA SOUVERAINETÉ NUMÉRIQUE: UN AUTRE ATTRIBUT DE L'ETAT BOUSCULÉ PAR LE TRANSNATIONALISME NUMÉRIQUE.

L'approche alarmiste des enjeux de l'internet plombe une lecture réaliste d'un fait social ayant acquis le plein statut de la totalité[82]. Elle qui considère internet comme la «plus grande expérience d'anarchie de l'histoire»[83]. Le cyberespace est plutôt une structure d'opportunités appropriable par la multitude des acteurs des relations internationales. L'Etat en réclame l'exercice de sa souveraineté que lui disputent les acteurs transnationaux. C'est dans les interstices de ce double attrait que se joue le jeu des appropriations.

A - L'ESSAI DE CAPTATION OU TERRITOIRE «NUMÉRIQUE PAR L'ETAT»

La souveraineté numérique est envisagée en termes de captation du cyberespace par l'Etat: elle suppose plus prosaïquement «l'extension de la République dans cette immatérialité informelle qu'est le cyberespace» et «l'expression sans entrave sur les réseaux numériques de la volonté

[81] Moine A., «Les aspirations à l'Etat au Califat de l'organisation Etat islamique», *Civitas Europa*, Vol.1, n°38, 2017, pp.127-152.
[82] Mauss M., *Essai sur le Don, Forme et raison de l'échange dans les sociétés archaiques*, Paris, PUF, 2007.
[83] Schmidt E., Cohen Jared, *The New Digital age*, op. cit., p. 11.

collective des citoyens»[84]. A souveraineté numérique revête le caractère de tout un projet de société voué à la «maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies des réseaux informatiques», écrit Bellanger.

L'approche juridique de la souveraineté numérique la réitère comme un attribut souverain de l'Etat, et conçoit l'action de ce dernier comme un prolongement du pouvoir général de réglementation qui s'étend sur le cyberespace. L'exercice de ce pouvoir est conçu selon les Etats tantôt comme un exercice sans entrave, tantôt comme le droit pour un Etat de «protéger ses citoyens et leurs libertés contre les entités malveillantes ou mues par des intérêts purement commerciaux». Cette approche juridique est ballotée par une approche économique et politique incarnée par le GAFAM qui se réclame d'un pouvoir de régulation du cyberespace[85] et une approche libérale qui est une reprise réchauffée de la théorie rousseauiste de la souveraineté populaire. Leur emprise sur l'intelligence artificielle pourrait, selon certains critiques, menacer la souveraineté des Etats[86].

Dans tous les cas de figure, il a une propension affichée des Etats à en avoir une conception westphalienne: propension bien plus crue pour la Russie et la Chine qui «revendiquent la restauration de leurs droits souverains sur la gestion du réseau et l'élaboration d'un traité international permettant de mieux partager les responsabilités»[87]. Ces derniers comme l'Iran, en fait d'ailleurs une conception autoritaire. Même si l'approche française et allemande est passablement libérale, elle traine une inquiétude sur la floraison des Hacking, fake news, du rançongiciel; d'où la position somme toute ambiguë de Michelle Alliot Marie qui en 2009, se propose de «garantir la souveraineté numérique et étendre à l'espace numérique le champ de l'Etat de droit»[88].

C'est surtout le cas USA qui suscite bien des critiques et non moins

[84] Bellanger B., *La souveraineté numérique*, Paris, Stock, 2014
[85] Le GAFAM ou encore le «Big Five» est l'acronyme des principaux web qui dominent le marché du numérique, notamment Google, Apple, Facebook, Amazon et Microsoft.
[86] Boussad A., *La face cachée de l'intelligence artificielle*, VA éditons, 2020.
[87] Bohamou B. et al, Comprendre la souveraineté numérique, Cahiers français, n°415, Mai-Juin 2020.
[88] In Untersinger M., «L'incertaine, mais nécessaire souveraineté numérique», le Monde, 20 novembre 2019.

d'inquiétudes en raison de son quasi-monopole à travers les grandes entreprises numériques (GAFAM, Uber, Tesla, Airbnd, Netflix) qui maitrisent tous les systèmes d'exploitation. Cette domination est monitorée par la société californienne ICANN (Internet Corporation for Assigned Names and Numbers), société à but non lucratif ayant pour mission d'administrer les ressources numériques d'internet notamment l'adressage IP, les noms des domaines de premier niveau (TLD) et la coordination d'acteurs techniques[89].

La peur de la perte de la souveraineté classique sur ces espaces virtuels suscite les plus vives appréhensions. Eric Sadin parle d'une «colonisation d'un nouveau genre qui ne se vit pas comme une violence subie». Il parle même de la «siliconisation» du monde[90]: ne se jouant plus dans les frontières physiques, se construisent dans le cyberespace des puissances multinationales qui rivalisent désormais l'Etat dans la gestion des sociétés humaines. Et c'est un remarquable d'humour que de voir le Danemark nommer un ambassadeur à la Silicon valley en 2017.

De cette irrésistible mutation, l'on peut tirer trois enseignements: d'abord la souveraineté post-westphalienne ne peut plus être pensée indissociablement de l'emprise qu'ont les multinationales sur le cyberespace: ensuite n'étant plus au siècle de Jean Bodin, de Charles Loyseau (18e siècle) ou de Louis de Fur et Raymond Carré de Malberg (20e siècle), les grandes «turbulences» actuelles nous inclinent à une appréhension combinatoire de la notion de souveraineté aujourd'hui moins «ultime et moins perpétuelle»: le défi étant celui d'un équilibre entre une approche juridique toujours hantée par la souveraine puissance de l'Etat, une approche politique et économique où les acteurs s'emploient à toujours exercer un pouvoir de commandement et de règlementation du cyberespace, et une approche libérale qui consacrerait la souveraineté des utilisateurs ou ce que P. Turk appelle l'»autonomisation informationnelle». Enfin, il y a une hiérarchie à trois échiquiers dans l'occupation du cyberespace: le premier tout naturellement occupé par les Etats-Unis à travers ses grandes

[89] «Who runs the internet?» (RNG), sur www.ICANN.org

[90] Sadin E., *La siliconisation du monde: l'irrésistible expansion du libéralisme numérique*, Paris, L'Echappée, 2016, p.24.

multinationales (UBER, TELSA, AIBNB, GAFAM) qui dominent le marché numérique sous l'appellation métaphorique de «Big Five». La conception politique et économique se révèle être un trait remarquable de l'approche américaine de la souveraineté numérique: d'autant plus que toute tentative de réglementation restrictive a toujours dans la vie politique américaine des effets dommageables pour les entrepreneurs politiques. Cette conception est d'inspiration libérale et s'accommode de la souveraineté populaire numérique.

Le deuxième échiquier est occupé par certains Etats européens qui globalement conçoivent la souveraineté numérique comme la capacité de l'Etat à agir dans le cyberespace, qui suppose «une capacité autonome d'appréciation de décision et d'action» dans ledit espace, et la maitrise «de réseaux, des communications électroniques et des données»[91]**.** La conception de la souveraineté numérique incarnée principalement dans le contexte européen par la France et l'Allemagne est incontestablement hybride, l'Etat étant au centre des politiques publiques numériques, et historiquement très marqué par la notion de puissance publique.

Dans le troisième échiquier, logent les Etats qui en riposte à la «siliconisation» du monde transposent les attitudes idéologiques dans le cyberespace. La montée en puissance de la Chine et de la Russie montre une volonté de contrôler sans entrave leurs espaces numériques. Cette conception est même ostensiblement autoritaire et ayant partie liée avec l'ordre westphalien, se fondant sur leurs «droits souverains» sur la gestion de l'espace numérique. La tendance consolidée affichée par l'Inde et le Brésil dans la création des moteurs de recherche et la mise en place des systèmes d'exploitation autonomes renforce cette tendance. En tout cas, pour la Russie et la Chine la souveraineté numérique constitue tout d'abord un enjeu sécuritaire.

Face à la toute-puissance américaine les auteurs privilégient une approche proactive et collaboratrice plutôt qu'une posture toujours «défensive et agressive»[92]: «nullement agressive et parfaitement

[91] Rapport de la commission d'enquête au Sénat français sur la souveraineté numérique, 2019.
[92] Alomar B., «Ne sombrons pas en Europe dans le nationalisme numérique», Lesechos.fr, 4 mars 2020.

inefficace», la souveraineté numérique selon Christophe Alexandre Paillard, est une politique «colbertiste»[93].

L'on pourrait se résoudre à une globalisation du numérique qui impliquerait selon Joseph Nye une gouvernance mondiale qui assure la protection des fonctions vitales d'internet, la résorption des cyber conflits et une offre de service plus démocratique[94]. Quelle que soit la puissance numérique d'un Etat, et la sophistication qu'elle peut charrier l'appropriation de cet outil par les acteurs autres que l'Etat le prédispose à «prendre l'eau»: le dispositif sécuritaire n'étant pas suffisamment étanche pour obstruer toutes les possibilités de piratage. Certaines organisations non gouvernementales à but non lucratif offrent une audience attentive aux lanceurs d'alerte et aux fuites d'informations dotant ainsi ces acteurs transnationaux d'opportunités d'actions qui assènent de sérieuses entailles au corps hermétique de l'Etat. L'ordre westphalien hiérarchique se trouve ainsi tancer par ces éléments perturbateurs qui hiérarchique en contrepoint d'un Etat fort, oppose un modèle réticulaire et décentralisé de subvention de la diplomatie internationale.

B - L'ORDRE WESTPHALIEN SUBVERTI PAR LE TRANSNATIONALISME NUMÉRIQUE: LE PARADIGME ASSANGE

Habermas définissait à la suite d'Emmanuel Kant, qui projetait l'idée d'un «espace public mondial», l'espace public en général comme ce processus au cours duquel le public constitué d'individus faisant usage de leur raison s'approprie la sphère publique contrôlée par l'autorité et la transforme en une sphère où la critique s'exerce contre le pouvoir de l'Etat»[95]. Ce processus qui date du 18e siècle s'est vertigineusement amplifié dans un contexte de mondialisation où les interactions humaines sont saisies par les TIC. Bernard Miege parle d'une «société conquise par une communication» dominée par les médias audiovisuels de masse[96].

[93] «La souveraineté numérique, un colbertisme 2.0?», sur Atlantico.fr, 24 mars 2020.
[94] Nye J., «Maîtriser les cyber conflits, sur project syndicate», 8 Août 2017.
[95] Habermas J., *L'espace public: archéologie de la publication comme dimension constitutive de la société bourgeoise*, Paris, Payet 1997.

Julian Assange insuffle à cette réalité une dynamique plus agressive. Il se déclare ouvertement en faveur de la transparence de l'information et du libéralisme économique.

Ce qui importe plus que cette «nouvelle forme numérique pour le journalisme d'investigation», c'est cette action inédite de subversion de la diplomatie internationale à travers des coups d'éclat médiatiques. Son postulat de l'asymétrie informationnelle entre les dirigeants et le peuple rend ambitieux son projet de défiance de l'Etat: puisque son objectif à long terme est de faire de wikileaks «l'organe de renseignement le plus puissant au monde»[97]. Ce culte de l'anti-souverain témoigne selon Baunan de la «liquidité» du Web: l'auteur du «liquid modernity» précise le sens de cette métaphore. «Les liquides contrairement ceux solides, ne peuvent tenir dans leurs formes. Les fluides pour ainsi dire ne fixent jamais l'espace, ni ne lient le temps. Tandis que les solides ont des dimensions spatiales claires, mais neutralisent l'impact, par conséquent dégrade la signification, les liquides fuient»[98].

Le paradigme «wikileaks» s'inscrit dans cette modernité liquide qui assène ses coups les plus fatals à la diplomatie du secret. Franck Petiteville, oppose - pour le bonheur de la métaphore -, un David cyber militant au Goliath (super puissance américaine). Un «*skillful indivisual*» opère une sérieuse entaille dans le dispositif rassurant de la diplomatie classique. Ce militantisme virtuel en rajoute surabondamment à une tendance qui se consolide depuis trois décennies par le «sans frontiérisme» humanitaire et l'accélération de la mondialisation[99]. Relevant d'une politique publique sui-generis soustraite au traitement ordinaire, la diplomatie classique va sous les corps de boutoir des révélations d'Assange parasiter le mythe de la confidentialité jusque-là considéré comme «un élément intrinsèque de la diplomatie»[100]. Franck Petiteville demeure à ce sujet intransigeant: «on ne

[96] Miege B., *La société conquise par la communication*, T1 et T21, Presses universitaires de Grenoble, Grenoble, 1996-1997

[97] Herbert M., «Wikileaks, une machine à scoops efficace, mais opaque», Lefigaro.fr, 26 juillet 2010.

[98] Bouman z., *Liquid modernity*, Cambridge, Cambridge polity press, 2000.

[99] Rufin J-Ch., «Wikileakes ou la troisième révolte, le Monde du 21 décembre 2020.

[100] Rivkin C., «La confidentialité est un élément intrinsèque de la diplomatie», Le Monde du 30 novembre 2010. Ce débat est relancé par Nathalie Labalme, «opinion publique et politique étrangère: l'évolution d'un débat» in Fréderic C. , (dir.), *Politique étrangère, Nouveau regards*, Paris, Presses de sciences politiques, 2002.

saurait… continuer à justifier le secret et la confidentialité de la diplomatie par un nécessaire statut dérogatoire de celle-ci par rapport aux règles démocratiques»[101]. En tout cas dans cette mouvance, l'auteur relève un «effet de relief» et un «effet de vitriol» qui fixent désormais l'azimut des rapports entre le diplomate et le citoyen.

Le «cablegate» du 28 novembre 2010 n'a certainement pas été le premier coup d'éclat de wikileaks. Parmi bien d'autres «faits d'arme», il avait déjà mis en ligne 31832 documents top secret sur l'aventure militaire irakienne, levant le voile sur un véritable massacre auquel se serait livrée l'armée américaine, jusqu'aux pratiques de la torture[102]. Mais au demeurant les révélations des télégrammes de la diplomatie Américaine sont impressionnantes. Ce sont 2 541 287 télégrammes qui sont diffusés: dans les effets de relief les plus saillants est pointée l'américanophilie de Nicolas Sarkozy qui se présente délibérément comme un adjuvant de la politique Américaine: bien plus, le cablegate révèle une défiance de Sarkozy au grand dam de la solidarité gouvernementale face au Président de la république française Jacques Chirac et au premier ministre sur l'invasion irakienne, position qu'il juge «injustifiable et excessive». S'étant résolument aligné sur la ligne dure de la droite américaine les révélations des câbles le juge «instinctivement pro-israélien, anti Obama et contre l'admission de la Turquie dans l'Union Européenne»: est révélé également à traits renforcés le caractère «corrompu du régime tunisien de Ben Ali: ainsi que les connections supposées de Berlusconi avec la Russie: jugé «incapable vaniteux et inefficace, le chef du gouvernement italien est «qualifié de porte-parole de Poutine en Europe».

Levant le voile sur la diplomatie du secret, Wikileaks passe au vitriol la politique étrangère américaine sous l'administration de Barack Obama, en révélant une directive signée de Hillary Clinton en 2009 instruisant les chancelleries américaines de procéder sans exclusive au glanage des «renseignements humains» sur les pays hôtes à travers les annuaires

[101] Petiteville F. , «Wikileaks ou la subversion de la diplomatie internationale» in Bertrand Badie et Dominique Vidal (dir.), *Nouveaux acteurs, nouvelle donne, L'Etat du monde 2012*, Paris, La Découverte, 2011.

[102] «Huge wikileaks release shows us ignored iraqi torture», sur BBC, 28 octobre 2021: «Wikileaks: guerre en IRAK: la coalition internationale a torturé des prisonniers», le point, 23 octobre 2021

téléphoniques, la liste des e-mails, les identifiants et mots de passe internet, carte de crédit, jusqu'aux données biométriques. Les câbles révèlent aussi une Russie «régressive vers une diplomatie étrangère tsariste, impérialiste, brutale, reflétant de l'antisémitisme et du nationalisme»: selon Jean-David Levitte, la Russie serait un «Etat révisionniste» qui considère qu'un «bon ami est un subordonné totalement soumis».

Nous sommes bien loin de l'«espion honorable» dont parlait Abraham de Wicquefort[103] pour célébrer les vertus de la diplomatie secrète: Wikileaks dévoile un diplomate fouineur des interstices de la vie privée. Les tractations de coulisse sont sur scène, montrant l'extrême capacité de nuisance des acteurs transnationaux dans leur manipulation experte du cyberespace. Par le «fil du social» se lit une société internationale profondément émasculée et dont Hillary Clinton s'alarmait du péril que cette dérive pouvait causer à la sécurité nationale des Etats-Unis[104] . La construction de la réalité internationale au travers du «Storytelling» et la déconstruction de la puissance classique à travers la «subversion de la diplomatie internationale», renseignent sur le monde réticulaire, décentralisé où la bataille médiatique fait émerger des allégeances concurrentielles aux Etats.

B - NOUVELLES ALLEGEANCES ET NOUVELLES STRUCTURES LEGITIMES

L'Etat-Nation mis à mal par les «turbulences», entraine une perturbation de l'encrage des groupes et des individus qui ne s'articulent plus aisément avec la culture nationale[105]. Bertrand Badie remarque que le modèle national d'inspiration occidentale se liquéfie sous l'effet «d'une double dysfonction: l'atomisation croissante des particularismes… et la coexistence des modes différents d'identification»[106].

---

[103] Wicquefort A., L'ambassadeur et ses fonctions, 1681, in Guillaume Devin, *Sociologie des relations Internationales*, La Découverte, 2007, p.45.

[104] La réaction a été d'ailleurs immédiate lorsqu'elle a ordonné le déménagement du Secret Internet Protocol Router Network monitoré par le Pentagone (voir les rapports secrets du département d'Etat Américain: le meilleur de Wikileaks, hors-série, le Monde, Février 2011.

[105] Taguieff PA et Delannoi G., *Théories du nationalisme,* Paris, Kimé, 1991.

[106] Badie B. et Smouts M –C., *Le retournement du monde: sociologie de la scène internationale*, op.cit., P.48.

Sans prétendre épuiser la foisonnante nomenclature des identités naissantes sous l'effet des turbulences internationales, l'on peut sérier deux formes contrastées sous deux régimes d'identification, exprimant mieux la perceptible segmentation des allégeances: nous distinguerons ainsi les communautés d'allégeance sub-nationales des communautés d'allégeance supranationales: les premières défiant l'Etat sur la scène internationale et les secondes le parasitant de l'intérieur, bien que pouvant avoir des répercutions à l'international. Les allégeances supranationales peuvent être vertueuses comme elles peuvent revêtir des formes d'expression violentes et criminelles.

1 - LES NOUVELLES ALLÉGEANCES SUPRANATIONALES

Les identités ont ceci de singulier qu'elles peuvent être choisies, imposées, subies ou suggérées[107]. L'allégeance citoyenne à l'Etat-Nation est apparue à travers les âges comme une identité subie, voire imposée. L'ordre Westphalien a été un ordre hégémonique en apesanteur sur une réalité sociale totalement étrangère aux traités en 1648 entre Ferdinand III, la France, la Suède et leurs alliés respectifs. L'histoire du développement politique occidental a, ainsi, enfermé les micro-identités dans le projet de construction d'une communauté nationale qui devait les pulvériser: ainsi les identités transnationales autres que celles suscitées par l'Etat étaient bridées au profit d'une solidarité organique à laquelle la nation devait donner une âme et une unité[108]. Aujourd'hui, la construction du nouvel ordre international démultiplie et complexifie, sans cesse, les particularismes[109] dont l'une des versions s'exprime dans l'allégeance supranationale vertueuse.

A - LES ALLÉGEANCES SUPRANATIONALES VERTUEUSES

[107] Bergeron J., Francophonie d'Amérique: Identité choisie, imposée ou suggérée: Francophonie Nord-américaine, n°9, 1999, pp. 143-156: voir aussi Charles Daniel Maire, *Identité subie ou identité choisie ?*, Olivétan, 2009.
[108] Durkheim E., *La division sociale du travail*, Paris, PUF, 2007.
[109] Badie B., op. cit., p.48.

Ce sont celles qui offrent aux acteurs une prédisposition à agir autrement que par la violence et supposent une cause et une certaine éthique de responsabilité et de conviction. L'on y retrouverait une communauté de croyance qui transcende les frontières étatiques et qui sustentent une identité fortement agissante: de même que pourrait y figurer les mouvements de la société civile internationale se revendiquant d'une cause «noble». Loin de commettre un anachronisme angélique, la vertu appartient au registre des représentations collectives d'une communauté valorisée à l'intérieur de ladite communauté. Il va sans dire que cette représentation peut ne pas être partagée par d'autres groupes sociaux: les convictions et les représentations de ces allégeances subissent un «effet de champ» qui fondent une solidarité d'intérêts symboliques[110]. L'on retrouve pareille allégeance dans sa forme la plus consolidée au sein de la Oumma (littéralement la nation islamique) née avec l'Hégire en 1622 et matérialisée dans la constitution de Médine. Dès ses fonts baptismaux, cette charte consacre un transnationalisme à travers un pacte entre les immigrés, les Ansars et les Juifs[111].

Même si certains auteurs considèrent ce texte moins qu'une constitution, que comme une proclamation unilatérale du prophète Mahomet[112], et bien plus malgré les ruptures successives dues à l'héritage du prophète, la Oumma a créé une allégeance transnationale tributaire d'une double protestation: contre les «Etats en place leur faible légitimité» et contre le modèle occidental de civilisation. Richard Mitchel souligne la transnationalité de la Oumma, qui se manifeste à travers un faisceau d'associations et de réseaux de fraternité qui témoigne d'un déplacement des allégeances citoyennes, une communalisation spirituelle. Le Jamaat al Tablik, le Jamiat al Ikhwan al Muslimin sont des réseaux associatifs et de fraternité qui transcendent les frontières territoriales et qui par ailleurs expriment l'acuité des crises identitaires[113]. Ces réseaux se posent même en «communautés de responsabilité», notamment de la responsabilité

[110] Bourdieu P., «Effet de champ et Effet de corps», *Actes de la recherche en sciences sociales*, année 1985, n°59, p.73.
[111] Nagel T., Mahomet, *Histoire d'un arabe: Invention d'un prophète*, traduction de Jean Marc Tetaz, éd. Labor et Fides, 2012, p.156.
[112] Lewis B., *The Arabs in history* (Traduction, les arabes dans l'histoire), Paris, Flammarion, 1996, P.42.
[113] Mouiche I., «Islam, Mondialisation et crise identitaire dans le royaume Bamoun (Cameroun)», Africa, volume 8, 2005.

sociale de l'investissement. Les théoriciens de l'économie islamique soutiennent que la finance islamique constitue la troisième voie entre le capitalisme et le communisme[114]: les banques islamiques foisonnent depuis 1956 et se chiffrent en 2012 à 1540 milliards de dollars: au point de s'imposer aujourd'hui comme une solution à laquelle s'accommodent désormais volontiers les Etats à travers une fiscalité souple[115].

La figure d'Oumma s'impose ainsi par l'obligation de privilégier l'épargne vertueuse et la prohibition de l'intérêt, et une claire définition des secteurs d'intérêt prohibés. Bien que critiquée[116], la finance islamique s'appuie sur une économie de la charité qui force l'adhésion d'une «communauté imagée» des croyants. Cette transnationalisation identitaire des finances islamiques recoupent les principicats de la finance catholique telle que l'analyse Antoine Cuny de la Verryère à partir des «Traités des vices» de la doctrine sociale de l'Eglise[117]. Religieusement connotées, les allégeances vertueuses peuvent prospérer dans un activisme laïc, notamment les allégeances protestataires altermondialistes.

B - LES ALLÉGEANCES PROTESTATAIRES ALTERMONDIALISTES

L'altermondialisme, aujourd'hui se présente sous une forme hétéroclite mêlant diversement Associations (ATTAC), ONG (OXFAM, WWF, Greenpeace, Handicap International), organisations de défense des droits de l'homme, des syndicats: l'hétérogénéité de ce mouvement se perçoit également dans son inscription idéologique: un mélange de communisme, d'antilibéralisme, d'écologisme, de localisme sous la bannière d'un apophtegme transnational prêchant la possibilité d'un «autre monde». Comme dans le Storytelling, les altermondialistes fabriquent leur histoire

[114] Sayyid Abdoul A'la M., *Economic Problem of man and its Islamic solutions*, ed. Lahore, Pak: Islamic Publications, 1975.

[115] La législation Britannique par exemple tient compte de la taxation des opérations de financement afin d'éviter la double taxation. Le Royaume Unis a même lancé une initiative de Sukuk très favorablement accueillie par les Britanniques.

[116] Gassama S. D., «La finance islamique dévoilée», Toulouse, 2014.

[117] Verryère Antoine Cuny de la , *La finance publique catholique: Au fondement de la finance éthique et solidaire*, EMS, Paris, 2013.

dans une articulation rhétorique qui appuie sa base lexicale sur l'«anti-mondialisme». Ils usent à profusion des médias et de nouvelles technologies d'information et de communication pour accroitre leur audibilité et leur capacité actantielle. L'altermondialisme draine une «clientèle jeune à niveau social et culturel élevé», et fonctionne sous un «mode d'organisation valorisant l'informel et les réseaux, avec les modes d'action ludiques et contestataires… et un engagement politique de gauche ou d'extrême gauche»[118]. En tout cas idéologiquement, l'altermondialisme incarne la conscience planétaire et tente de fédérer toute la «galaxie anti-globalisation»[119], s'offrant ainsi comme le parlement de l'»intérêt général mondial».

Loin d'être un système d'irradiation solaire, l'altermondialisme est une nébuleuse, il fourmille en groupes et en Associations indociles. Ces actions s'inscrivent dans un mouvement de transgression sacrilège pour l'ordre Westphalien. Ils provoquent, défient, émasculent: par le slogan - un autre monde est possible -, ils organisent ce que l'on pourrait appeler en pastichant les anthropologues, «une inversion sociale internationale». L'altermondialisme forme une catégorie toute particulière d'allégeances supranationales vertueuses. En effet, la boîte à outil idéologique de ce mouvement renferme des thématiques transportant une forte condensation sensorielle: refusant la mondialisation libérale et ses excès, il propose un syncrétisme idéologique mêlant plusieurs sources d'inspiration. Sont décriés l'accroissement des inégalités mondiales et locales, la dégradation de l'environnement, l'injustice sociale, le dictat des grandes instances internationales libérales, la domination des supers puissances et ses firmes transnationales sur les pays pauvres. Leur moyen d'action associe le ludique, le symbolique, le rituel carnavalesque: bref, tous les «ingrédients de l'«inversion sociale»[120].

Tous les répertoires d'action symbolique sont mobilisés jusqu'à la

[118] Meyer N., Siméant (Johanna), «L'espace de l'altermodialisme», *Revue Française de Science Politique*, n°54(3), 2004, pp. 373-378.
[119] Sommier I., *Le renouveau des mouvements contestataires à l'heure de la mondialisation*, Paris, Flammarion, 2003, pp.318-319.
[120] Perrot C. H., «Le rituel d'inversion dans le Agni de l'Indénié», *Cahiers d'Etudes africaines*, n°27, 1967, pp.434-443.

fiction. Ainsi, la filmographie de l'altermondialisme va se ressourcer dans les multiples coups d'éclat de ces objecteurs de conscience. «Bataille à Seattle», par exemple, est une fiction basée sur les manifestations lors du sommet de l'OMC: «un crime d'Etat» de Danielle Vicari ajoute un effet de relief à la répression des manifestations altermondialistes contre le G8 de Gènes en 2001: ou la «Belle verte» de Coline Serreau (1996) qui met en scène une fable écologiste utopiste. Sans exhaustivité, l'on pourrait également citer une adaptation cinématographique de l'œuvre de Jean François Brient par Victor León Fuentes qui dans»de la servitude moderne» décrit le monde contemporain comme un totalitarisme marchant, dénonçant ainsi la condition d'esclave de l'homme[121].

C'est sous ce soubassement social et symbolique que les altermondialistes diffusent leur contreculture. Ils organisent des manifestations contre le travail des enfants (La société Nike en 1997), s'opposent aux FTN agroalimentaires producteurs d'OGM. Les Igloos et les Yourtes qu'ils installent à l'avant-veille du sommet de Davos en Suisse renvoient à une sorte de «cauchemar de Darwin» contre l'évolutionnisme moderne auteur des drames écologiques. Leur arrogance symbolique s'exprime parfois dans des rassemblements spectaculaires qui très souvent confinent les chefs d'Etat et Gouvernements à une diplomatie de barricade: aussi procèdent-ils ces derniers temps par défiance, à un dédoublement institutionnel symbolique où le Forum Economique Mondial est dupliqué d'un Forum Social Mondial organisé à juste titre à Porto-Alegre au Brésil: expérience qui se démultiplie sur tous les continents.

En dehors de l'altermondialisme, l'on pourrait évoquer le «printemps arabe» qui bien que ne visant pas particulièrement l'Etat, mais sa gouvernance, a par effet «Spill over», traversé les frontières étatiques de la Tunisie au Bahreïn. Il est à noter que la rapidité de diffusion de ces soulèvements a été dans une mesure significative le résultat de l'usage de TIC par la jeunesse. En l'absence d'un leadership politique, les TIC ont exercé une fonction réticulaire dans la diffusion des thèmes de la révolte

[121] Il s'inspire sans doute du «Discours sur la servitude volontaire» d'Etienne de la Boétie dont le thème défendu décrit la condition paradoxale de la servitude: «Si cette servitude perdure, s'il existe des maitres, c'est parce que les esclaves ont choisi de demeurer esclaves et non parce qu'il existe des maîtres».

aussi bien que le rôle mobilisateur d'Al Jazeera et des médias traditionnels. Cette fièvre obsidionale est un mouvement cosmopolite[122] qui secoue dans le monde arabe l'ordre post Westphalien. N'étant pas doué d'une capacité structurelle permanente, le «printemps arabe» peut, dès lors, être classé dans la catégorie d'actions porteuses d'allégeances spontanées: plus hardies dans la dynamique de perturbation de l'ordre post Westphalien sont les catégories criminelles et primordialistes.

2 - LES ALLÉGEANCES CRIMINELLES ET PRIMORDIALISTES

Le distinguo entre allégeances criminelles et allégeances primordialistes renseigne sur le caractère transnational des premières et singulièrement sub-étatique des secondes. Charles Tilly considére comme tragiquement pertinente, l'«analogie entre la pratique de la guerre, la formation de l'Etat d'une part, le crime organisé de l'autre»[123]. Il est de plus en plus factuellement prouvé que la structuration spatiale des Etats est sujette à un activisme transnational informel ou illicite, où banques, entreprises, filières criminelles assurent la fongibilité du légal et de l'illégal. La criminalité dont il est question ici a trait aux entreprises de violence que conduisent les islamistes dans la mise en crise de l'Etat post Westphalien.

A - TRANSNATIONALISATION DE LA VIOLENCE ET ALLÉGEANCES CRIMINELLES

L'on aurait tort de ne pas faire le départ entre le jihadisme violent et la criminalité organisée. Le jihadisme est d'ordinaire mu par l'idiologie salafiste qui prêche un retour aux «pieux ancêtres» et une interprétation fidèle des saintes écritures, induisant ainsi un rejet systématique des innovations religieuses. Il y a donc chez les jihadistes une violence sustentée par une vision du monde: toute chose qui ne motive guère les professionnels de la criminalité organisée. Toutefois dans la pratique, cette

[122] Gelabert E., «Le printemps arabe est perspective», *Cahiers de l'action*, vol. 2, n°39, 2013, pp.11-17.
[123] Tilly C., "War Making and state Making Organized Crime" in PB Evans, Ruesher Meyer and T. Skocpol, (Ed. Bringing the State back, Cambridge, Cambridge university Press, 1985, P.186.

frontière apparait labile et contrarie quelque peu les jihadistes dans l'accomplissement de leurs idéaux[124]. Le transnationalisme des mouvements jihadistes s'opère dans la banalisation des frontières étatiques et surprend par une ubiquité d'actions violentes instantanées dans plusieurs Etats: le Boko-Haram s'est constitué ainsi une ceinture jihadiste autour du bassin du Lac Tchad, circulant d'un pays à un autre avec une mobilité que le système sécuritaire des Etats n'arrive pas à obstruer. Leur légitimité tient à une idéologie hybride associant salafisme, takfirisme et anticolonialisme qui les inclinent à frapper d'apostats non seulement les tenants de la culture occidentale, mais aussi les formes modérées de pratique de l'Islam. Les groupes jihadistes érodent l'Etat dans ces fondements existentiels, «ruinent la fonction centrale de la paix et de sécurité… modifient la doctrine classique et commandent les agendas sécuritaires nouveaux et originaux»[125].

Ils le font avec un usage professionnel des TIC qui impacte l'opinion publique internationale. Et comme l'indique Omar Al-Ghazzi, «la médiatisation de la brutalité est une des principales stratégies pour terroriser l'ennemi»[126]: d'une manière générale, relève Denis Bauchard «des groupes jihadistes utilisent les formes les plus sophistiquées de la communication: les attentats sont soigneusement choisis en terme de lieu ou de date, et s'accompagnent souvent d'une mise en scène à travers des vidéos postées sur internet et sur les réseaux sociaux»[127]. Défiant les frontières de l'Etat post Westphalien, ils portent l'estocade transnationale jusqu'à la création d'un Etat: l'Etat étant conçu tout simplement comme une étape provisoire vers le califat. L'Islam salafiste - faut-il le souligner -, vise une application orthodoxe de la religion hors champ politique «en délaissant généralement celui-ci»[128].

En tout état de cause, l'Etat islamique a «pour vocation d'être universel

[124] Mandjem Y. P., «Les groupes jihadistes et les relations internationales: Contribution à une sociologie d'un acteur controversé (le cas du Boko Haram dans le bassin du Lac-Tchad», *Cahiers Thucydide*, n°27, 2020, pp.1-58.
[125] Mandjem Y. P., op. cit., p.6.
[126] Al-Gazzi O., «Modernity as a false Deity: Tackfiri anachronism in the Islamic state Group's Media Strategy», Javnost: the public, vol. 25, N°4, 2018, P.379.
[127] Bauchard D., «Géopolitique du jihadisme», *Questions Internationales*, Septembre-Octobre 2015, P.12.
[128] Ouardi H., «De l'autorité en Islam», *Le Débat*, 2012, N°17, P.168.

et global. Il représente le côté obscur de la mondialisation: il a le même public, la même audience, la même cible, mais propose une alternative à ce qu'il voit comme hégémonie occidentale»[129].

Les mobilisations primordialistes ont sans doute la même audience, et construisent leur discours sur la crise de l'Etat-Nation.

B - LES ALLÉGEANCES PRIMORDIALISTES ET CRISE DE L'ETAT-NATION

Les allégeances primordialistes s'appréhendent généralement à travers le prisme de l'ethnicité en raison de leur fort ancrage social. La croyance subjective à la communauté d'origine qu'elle sous-tend[130] tient potentiel de symbolisation que l'esprit humain investit dans la construction de la réalité sociale. Cette réalité construite nous installe dans des utopies et des illusions porteuses d'«effets de croyance»: illusions somme toute réalistes dont la logique de composition est tributaire des crises identitaires que charrient les dynamiques d'éclatement culturel imposées par le temps social. L'Etat-Nation, ce «veau d'or» du développement politique occidental, allait subir un éclatement d'allégeances suscitées par des dynamiques sociales horizontales dont les plus indociles seront incarnées par les identités ethniques et culturelles. Bertrand Badie trouve dans ce processus une double implication internationale: d'une part les allégeances nouvelles ainsi recréées sont retirées de l'espace de la citoyenneté, et d'autre part elles sont mises à la disposition d'organisations qui «acquièrent par ce biais une capacité transnationale»[131].

Les allégeances subnationales primordialistes n'émasculent pas l'Etat seulement dans son être endogène, mais administre une capacité de bifurcation internationale. Dans la crise anglophone au Cameroun par exemple, «il ne s'agit plus seulement, d'une négociation expurgée de sérénité qui donne à voir un épuisement du référentiel monopolistique de

[129] Atran S., *L'Etat Islamique révolution*, Paris, Liens qui libèrent, 2016.
[130] Weber M., cité par P. Pouginat et J. streiff-Fenart, *Théories de l'ethnicité*, Paris, PUF, 1995, p.38.
[131] Badie B., Smouts M –C., *Le retournement du monde*, op.cit., p.50.

l'Etat»[132], mais aussi la projection d'un conflit qui se mue insensiblement en séparatisme, avec des manifestations internationales qui compliquent l'implémentation des résolutions du Dialogue National.

La survie de l'Etat est ainsi ballotée dans la confrontation entre unionistes, fédéralistes et sécessionnistes. Cette lutte prend inattendument un tour de sacralisation caricaturale à travers un déplacement territorial des enjeux, du «champ» politique au «champ» religieux. Dans le contexte camerounais, les allégeances ne gravitent plus seulement autour de la triade unioniste / fédéraliste / séparatiste, mais aussi autour d'un sacré qui offre aux revendications une confortable hospitalité-refuge: par transmutation, des «sujets de la République» deviennent des «sujet de Dieu»[133].

En Republique Démocratique du Congo, sous une forme plus complexe, les expressions identitaires se sont intriquées dans un complexe conflictuel marqué par la défiance à l'Etat Westphalien à travers la banalisation des frontières internationales, où s'affrontent sept armées d'Etats voisins (Angola, Zimbabwe, Burundi, Ouganda, Rwanda, Namibie, Tchad). La criminalité internationale s'opère dans une imbrication des réseaux ethniques et leurs soutiens étatiques dans les provinces Nord et Sud Kivu, et dans le Maniema au détriment de l'Etat congolais dont le flanc Est constitue une base arrière pour les rebelles de toute la sous-région.[134].

Cette fluidité identitaire ne doit pas s'apprécier comme un stigmate afro-centrique puisqu'en Europe les singularités s'institutionnalisent et s'imposent à l'intérieur de l'Etat et sur l'échiquier international. La question «corse» et irlandaise, le réveil des ligues régionales Italiennes en Lombardie en Vénétie, et plus récemment le Mezzogomo, la question Kurde, le revivalisme hindou, le soulèvement des rebelles Chiites Houtis témoignent de son expansion planétaire. En Europe, la question irlandaisedevient même une hantise, où les minoritaires nationalistes tous catholiques réclamant

[132] Keutcheu J., «La crise anglophone: entre lutte de reconnaissance, mouvements protestataires et renégociation du projet hégémonique de l'Etat» *Politique et Société*, Volume 40, n°2, 2021, pp.3-26.
[133] Machiikou N., «Utopie et Dystopie ambazonniennes: Dieu, les dieux et la crise anglophone au Cameroun», *Politique Africaine*, 2018/2, n°150, pp. 115-138.
[134] Braeckman C., «République Démocratique du Congo: Un Etat post-conflit qui peine à se stabiliser» in Bertrand Badie et Dominique Vidal (dir.), *Nouveaux Acteurs, Nouvelle donne: l'Etat du monde 2012*, Paris, La Découverte, 2011, pp.222-228.

l'égalité des droits, s'opposent aux majoritaires unionistes protestants partisans du *statu quo*[135]. Lors du Bexit les nationalistes d'Irlande du Nord ont demandé un vote sur la réunification de l'Ile[136].

Tous ces mouvements, selon leur orientation, créent des communautés d'allégeances sub-nationales et supranationales contribuant ainsi à la mise en crise de l'ordre post-Westphalien.

CONCLUSION

L'ordre westphalien a exercé un «monopole dur» sur les Relations Internationales. Nous avons montré que cet «Ordre» a érigé l'Etat au pinacle d'une «statolatrie» nimbée par les principes juridiques qui ont consacré sa puissance et son exclusivité sur la scène internationale. C'est dans l'environnement historique de l'après-guerre de Trente ans que les traités de Westphalie consacrent cette puissance et qu'émerge la théorie réaliste qui a justifié la pertinence de l'institution étatique comme société politique irréductible. Vont apparaître dans cette quiétude souverainiste, et sous l'effet disruptif de la mondialisation, les linéaments d'une émasculation du corps hermétique de l'Etat. L'ordre westphalien fragilisé, est plus que banalisé par une bataille médiatique qui s'apprécie dans la capacité d'investissement des médias traditionnels et surtout du cyberespace par les Nouveaux Acteurs Transnationaux qui construisent des récits de vérité, et aménagent des espaces où s'engouffrent les nouvelles allégeances et les nouvelles structures légitimes. C'est en ce sens que le «retournement du monde» a partie liée avec la «réticularisation» du monde.

[135] Aufrechter F., «Irlande du nord): au-delà des divisions», *Journal International*, 8 Septembre 2013.
[136] Enora O., «Les nationalistes du Nord demandent un vote sur la réunification de l'Ile», Le Monde du 24 Juin 2016.

CYBERESPACE ET CRYPTOMONNAIE: ENJEUX, DEFIS ET PERSPECTIVES

Georges BELL BITJOKA
Professeur, Enseignant-Chercheur à l'ENSP, ENAM, Cryptologue,
Expert judiciaire en cybercriminalité

INTRODUCTION

Le cyberespace numérique s'est positionné aujourd'hui comme quatrième dimension géopolitique avec des changements majeurs qui nous imposent une adaptation rapide et bien étudiée nous permettant de garder le cap sur l'évolution de la société humaine. Le sujet que nous abordons dans le cadre de cet évènement est «cyberespace et cryptomonnaie: enjeux, défis et perspectives».Notre approche nous amène à repartir la question en deux parties, pour permettre une bonne lecture des analyses. Ainsi à la Partie1, nous commencerons par essayer de comprendre le cyberespace, sa perception et ses modèles, puis ses enjeux et perspectives. Et en partie2, nous parlerons de la crypto monnaie dans le cadre du cyberespace, son rôle, ses enjeux et perspectives.

I - CYBERSESPACE ET ENJEUX

Le terme cyberespace se comprend par deux expressions simples: CYBER et ESPACE

- L'expression CYBER désigne l'Immatériel ou l'Informationnel
- L'expression ESPACE désigne une Zone ou Environnement d'actions et d'interactions

Le CYBERESPACE se comprend donc comme une zone, ou un

environnement d'actions et d'interactions immatérielles ou informationnelles. C'est donc un espace de modélisation, de conception et de représentation abstraite des éléments réels et irréels de l'existant naturel. Dans cette première partie de notre texte, nous allons aborder les questions suivantes liées au cyberespace.

Questions-problème :

1. D'où nous vient donc la perception du cyberespace?

2. Est-il une création de la technologie ou celle de la nature?

3. Quelle configuration peut-elle prendre?

4. Quels sont les enjeux autour de ce nouvel espace géostratégique?

5. Quel est le rôle de la confiance dans cet environnement et par quelles fonctions garantit-on cette confiance?

ESSENCE DU CYBERESPACE

L'INFORMATION À LA BASE DU CYBERESPACE

L'information selon les cybernéticiens se définit comme: La preuve d'un phénomène, processus ou évènement dans la nature. Elle se caractérise par plusieurs propriétés. Elle peut être appréciée sous ses aspects qualitatifs (la norme de la langue, les points d'unicité, la véracité, la complétude, etc.…voir linguistique, sémiologie etc…) et quantitatifs (la quantité de l'information, l'entropie de sa source…voir informatique mathématique et télécommunications)

L'INFORMATION ET CHAMPS INFORMATIONNELS

L'information se diffuse comme l'énergie du milieu le plus fourni vers le milieu le moins fourni et est gouverné par la loi des équilibres quantitatifs et qualitatifs (c'est-à-dire: des milieux informationnels différents mis ensemble après un certain temps deviendront par diffusion informationnel identiques). L'information existe sous forme de champs informationnels qui forme des couches dans son cycle d'évolution.

COUCHES DU CYCLE INFORMATIONNEL UNIVERSEL

- La couche de données;

- La couche de connaissances;
- La couche de savoirs;
- La couche de croyances;
- La couche de confiance;
- La couche de conscience.

L'information dans son cycle peut donc former plusieurs cyberespaces, mais les plus connus sont;

- le cyberespace naturel (comporte tous les éléments et fonctions immatériels naturels: l'amour, la haine, les envies, les désirs, la volonté, le beau, la sympathie, etc…..);
- le cyberespace numérique (comporte les éléments et fonctions immatériels crées par interaction dans les machines à calcul numérique).

CYBERESPACE NUMÉRIQUE

Par analogie au cyberespace naturel et en copie à celui-ci, le cyberespace numérique repose sur un support technico-infrastructurel et est composé d'interactions et d'actions numériques abstraites liées aux opérations de traitement, transmission et conservation de l'information numérique. Le développement des réseaux informatiques et de télécommunications et leur globalisation a permis une extension de ce cyberespace au-delà des frontières d'une machine à calculer numérique, ou d'un réseau local de transmission jusqu'à la dimension globale ignorant complètement les frontières géographiques des pays. Comme pour le cyberespace naturel, le cyberespace numérique a une structure en couche:

- **La couche de données:** déjà en formation, elle représente l'infosphère (l'ensemble des données générées dans cet espace) et est exploitée en psychographie, profilage politique et marketing etc.... Elle représente la cible privilégiée des géants des réseaux sociaux et est leur fond principal de commerce. Elle est à ce jour le plus grand stock d'actifs numériques au monde. C'est elle qui fait la force de Facebook, WhatsApp, etc…
- **La couche de connaissance:** elle est juste en train d'entamer sa phase d'initiation, mais fait déjà l'objet des grandes convoitises et le terrain des grandes batailles géopolitiques et économiques. Avec le développement de l'intelligence artificielle, et la capacité de collecte de grande quantité

de données, les sciences de données permettent de créer la connaissance qui donne un grand avantage concurrentiel sur les plans économiques et géostratégiques;

- **La couche de savoirs:** en gestation, son influence est planifiée dans une quinzaine d'année, mais ce développement est conditionné par l'uniformisation culturelle. Cela explique la guerre des contenus culturels dans le cyberespace pour avoir le maximum d'influence au niveau de cette couche. Les applications sont déjà perceptibles dans la facilitation de l'orientation des croyances.
- **La couche des croyances:** aussi en gestation, mais agit déjà dans le cadre de l'influence numérique des leaders d'opinions et des managers de communautés numériques. Elle représente la dernière étape à la formation de la couche de conscience numérique.
- **La couche de confiance numérique:** elle est soutenue par les fonctions de confiances cryptographiques qui apportent les garanties de signature numérique, certification numérique, authentification, non-répudiation et même confidentialité.
- **La couche de conscience numérique:** c'est le saint graal du cyberespace, c'est l'espace de tout contrôle et de la toute-puissance espérée par les architectes du cyberespace numérique.

A la fin de cette première partie, nous pouvons tirer quelques leçons sur le cyberespace:

- espace économique, car riche en activités;
- espace social car crée la rencontre entre nous dans des modèles de sociétés et de communautés;
- espace d'influences diverses;
- espace d'existence;
- espace de conscience.

II - CRYPTOMONNAIE DANS LE CYBERESPACE: ENJEUX ET PERSPECTIVES

1 - CRYPTOMONNAIE ET CONFIANCE

La monnaie est un élément de change, un instrument de conversion de

valeur lors des échanges commerciaux. A ce titre, elle fait partie des outils de la couche de confiance, au même titre que la certification, la signature et bien d'autres. Pour comprendre donc la monnaie, il faut comprendre la notion de confiance et celle de chaines de confiance.

2 - RAPPELS SUR LA COUCHE DE CONFIANCE DU CYCLE INFORMATIONNEL DU CYBERESPACE

- 5eme couche du cycle informationnel, elle garantit les bases d'échanges et d'interactions dans le cyberespace;
- elle se matérialise sous forme de chaines de confiance selon deux modèles: (La chaine de confiance verticale et la chaine de confiance horizontale);
- dans le cyberespace numérique les fonctions de confiance sont fournies par la cryptographie.

LA CHAINE DE CONFIANCE VERTICALE

Basée sur une autorité de confiance racine et unique qui étend la confiance vers d'autres nœuds de confiance sur un modèle de chaine privée. Dans ce modèle, on ne peut vérifier que le nœud le plus proche. S'il y'a ruptures dans un nœud de confiance antérieur, la chaine peut être compromise sans que les entités n'en soient informées. Et si un nœud se compromet, presque toute la chaine de confiance sera corrompue.

Pour faire confiance à une entité dans la société, on est obligé de consulter l'autorité de confiance. Et si cette dernière est compromise ça devient une situation de corruption et de faux généralisé. Dans cette situation les valeurs échangées perdent complètement leur contenu.

Exemple: L'Etat qui repend la confiance dans les documents comme (pièces d'identité: la monnaie, les diplômes etc…)

- Ce modèle est couteux et risqué pour l'utilisateur;
- il ne peut pas s'appliquer dans les conditions d'échange intensifs comme l'échange d'information;
- impossible de vérifier toute la chaine de confiance, d'où le risque d'accepter le faux et la falsification;
- ce modèle permet de construire les PKI.

CHAINE DE CONFIANCE HORIZONTALE

Pour ce modèle de chaine de confiance, nous observons les propriétés suivantes :

- Il n'y a pas d'autorité de certification unique;
- tout le monde vérifie tout le monde et concours à la crédibilité de tout le monde par des actions d'opinion et d'accréditation;
- la confiance est distribuée de manière presqu'équitable auprès de toutes les entités de la société;
- pas de centre de certification unique et donc pas de risque de saturation du système de certification lors des grands échanges;
- usage permanent du consensus
- système moins couteux;
- moins de risque de corruption lors des échanges;
- chacun donne son appréciation sur les valeurs échangées et certifie ses actions dans un nœud d'échange public;
- tous les nœuds de confiance peuvent être vérifiés par chacune des entités, ce qui limite l'acceptation du faux et de la falsification.
- Ce modèle est à la base de la blockchain.

BASES DE LA CONFIANCE CRYPTOGRAPHIQUE

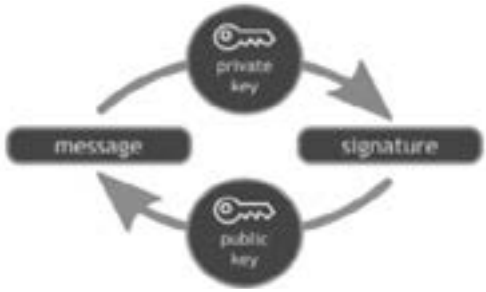


Figure N°1: Synoptique de signature et certification numériques (source: https:/WWW.senat.fr)

La cryptographie apporte les fonctions de confiances qui permettent au cyberespace numérique de bénéficier des propriétés suivantes :

- Authenticité
- Non-répudiation

- Intégrité
- Transparence/confidentialité

TOKENISATION COMME EXTENSION DE SOLUTION DE STABILISATION DE LA VALEUR MARCHANDE

Dans le but d'authentifier un élément physique ou numérique changeable, on l'associe à un jeton numérique correspondant appelé TOKEN. Cela signifie que les jetons sont utilisés pour lier les éléments physiques et numériques changeables à une chaine de block dans un système de confiance. Ces jetons numériques (appelés «tokens») sont utiles pour la gestion de la chaîne d'approvisionnement, la propriété privée digitale, la détection de la contrefaçon et de la fraude, mais aussi la fixation et la vérification des éléments de valeur de change ainsi que l'authentification de tout le système de change. Ce système est à la base de la cryptomonnaie, lorsqu'il est appliqué dans une chaine de confiance horizontale de type blockchain.

Énumérons ci-dessous quelques propriétés de la blockchain permettant de comprendre la cryptomonnaie;

DÉSINTERMÉDIATION

C'est la propriété la plus connue, à savoir la suppression du tiers de confiance qui se trouve remplacé par la technologie. En réalité, il serait plus exact de dire que la place des tiers de confiance va être déplacée et évoluer, sans toutefois disparaître Ainsi, les échanges se font directement de pair-à-pair entre les participants, et c'est le réseau qui valide les transactions grâce à un mécanisme de consensus.

RÉSILIENCE

La blockchain est partagée et répliquée sur tous les nœuds du réseau. Grâce à cette démultiplication de l'information, le système apparait résilient contre certaines pannes: si un nœud du réseau devient défaillant, les autres nœuds restent disponibles et le service continue à être rendu. A l'inverse, dans une architecture centralisée, si le nœud central tombe en panne, l'ensemble du système s'écroule.

TRANSPARENCE

Le contenu de la blockchain est validé par des membres du réseau grâce à un mécanisme de consensus, ce qui impose une certaine transparence dans le système. Cette transparence n'est toutefois, pas complètement incompatible avec la notion de confidentialité.

IMMUABILITÉ

La blockchain est une structure de données dans laquelle on peut rajouter des informations, sans pouvoir en soustraire: une fois qu'une transaction est inscrite dans la blockchain, elle ne peut en principe être retirée. C'est l'utilisation d'outils cryptographiques, associée au consensus, qui garantissent cette propriété d'immuabilité.

AUTOMATISATION

Sans être une propriété fondamentale de la blockchain, elle est particulièrement mise en avant dans les nouvelles générations d'implémentations. Ainsi, les transactions peuvent être automatiquement déclenchées lorsque des conditions prédéfinies sont remplies, sans intervention humaine et sans possibilité d'en empêcher l'exécution.

LES SYNOPTIQUES CI-DESSOUS MONTRE LE FONCTIONNEMENT D'UNE BLOCKCHAIN

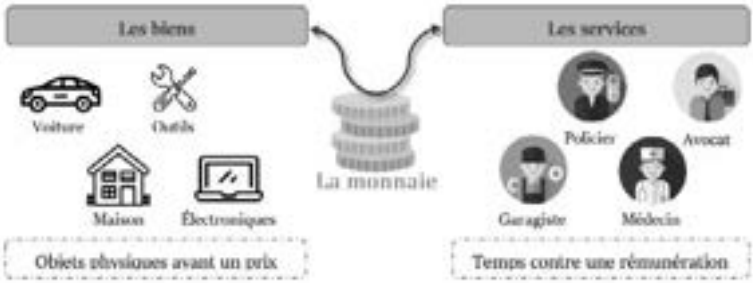


Figure 2: Synoptique de fonctionnement d'une blockchain (source: https:/changethework.com/blockchain-ressouces-humaines-2)

Le schéma ci- dessus montre le chainage, la signature et la publication des blocks dans un registre, de ces opérations naissent toutes les propriétés de confiance de la blockchain nécessaires à la production de la monnaie et d'autres structures de la chaine.

Dans le contexte de la blockchain, la monnaie est simplement considérée comme une écriture de valeur dans un jeton, qui introduit dans la blockchain portera toute les propriétés liées à cette dernière. Il y va également de tous les autres actifs cryptographiques comme les chaines de cryptofinance et les NFT.

Les synoptiques suivantes présentent les opérations dans la blockchain à crypto monnaies.

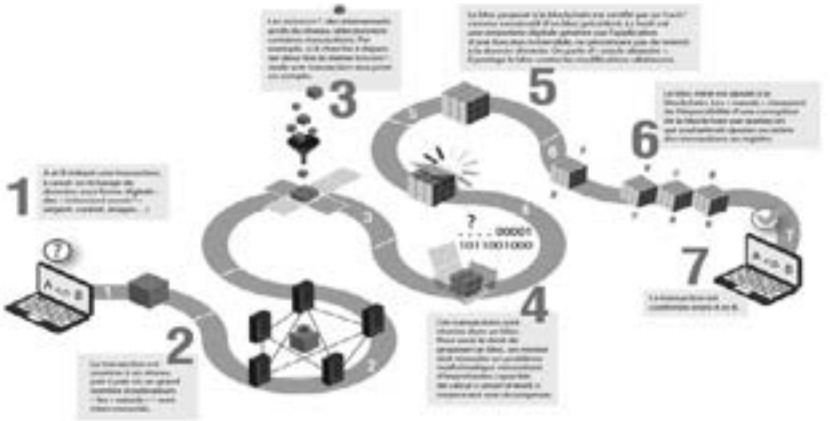


Figure N°6: Opérations cryptomonaies dans une blockchain (source: https:/WWW.institutdesactuaires.com/magazine/article/schéma-de-fonctionement-de-la-blockchain/2371)

La figure ci-dessus montre les opérations en cryptomonaies. On y voit bien les différentes opérations réalisées à chaque étape

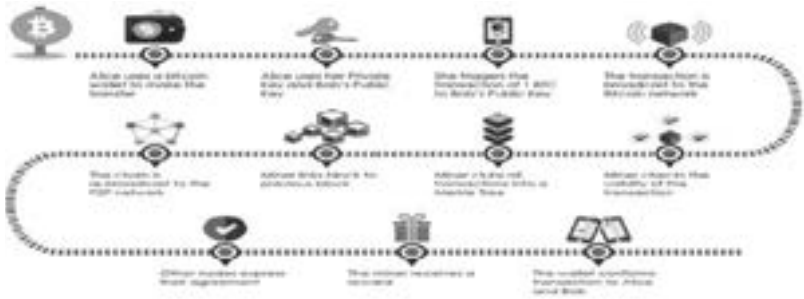


Figure N°7: Cycle de transactions cryptomonaie (source https://cryptomonaie.pro/quest-ce-que-la-crypto-monnaie/)

Le cycle ci-dessus décrit de manière détaillée les étapes de laréalisation des opérationsdans les transactions en crytomonnaies.

AVANTAGES DES CRYPTOMONNAIES

Ne dépendent pas des politiques monétaires des pays dont ne sont pas concernées par des sanctions et restrictions politiques:

- infalsifiables;
- non dévaluables par décision politique;
- non répudiables;
- transactions intègres;
- transactions faciles;
- globales et facilitent les levées de fonds;
- engendrent une très grande communauté financière libre et indépendante.

PROBLEMES

- Transactions parfois secrètes, pouvant faciliter le financement d'activités illégales et le blanchiment de capitaux;
- trop de spéculation sur les systèmes financiers autours de actifs y liés;

- carences de régulation entrainant un grand désordre;
- système assez libre pour inquiéter le contrôle politique.

Nous observons que les cryptomonnaies prennent de la valeur et sont de plus en plus adoptées par des nations comme le montrent les synoptiques ci-dessous;

Figure N°8: Marché de la cryptomonaie en 2021 (source: coinGekeo 2021)

Dans cette répartition des parts de marchés de la cryptomonnaie en 2021, on voit clairement les tendances et la dynamique du marché encore mené par le bitcoin, mais aussi la montée d'autres cryptoactifs basés sur ethereum, binance coin et autres, sur un marché global de plus de 3000 Milliards de Dollars américains.

Dans ce graphique, il apparait clairement les mouvements oscillatoires de la valeur du bitcoin sur quelques années, ce qui montre l'aspect spéculatif du marché du bitcoin, provoqué par les mouvements de l'offre et de la demande en cryptofinance.

Figure N°10: Adoption des cryptomonnaies et usage par pays (source: statista 2021)

Dans ce graphique on voit bien que l'usage des cryptomonnaies grandit dans plusieurs pays du monde et que ce type de monnaies est le plus adopté. Ceci s'explique par le fait que les cryptomonnaies nous offrent des opportunités et perspectives suivantes entre autres :

- La consolidation de la Propriété privée digitale;
- le Développement des Metaverses;
- la Globalisation et l'uniformisation de la valeur monétaire;
- le Marché de crypto finance et crypto monnaies est en pleine grandissant.

CONCLUSION

Les leçons que nous tirons de l'émergence et la montée en valeur des cryptoactifs et au vu de la situation de notre système monétaire et financier, il est plus opportun pour nous au Cameroun et en Afrique de :

- Etudier;
- réguler;
- adopter.

Pour le Cameroun, nous avons plus à gagner dans les cryptomonnaies, car elles nous libèrent de plusieurs contraintes monétaires et financières auxquelles nous sommes soumis, et nous donnent plus de liberté et d'opportunités dans nos objectifs de développement.

L'UTILISATION DES MEDIAS SOCIAUX PAR LES GROUPES TERRORISTES ET SECESSIONNISTES: DYNAMIQUE ET STRATEGIES DES ACTEURS

Brice MIMBOLO
Lieutenant-Colonel
Chef du Service des Renseignements à la Gendarmerie Nationale

INTRODUCTION

Depuis les attentats du *World* Trade *Center,* le 11 septembre 2001, aux Etats-Unis d'Amérique, le monde est entré dans une ère de banalisation de la violence par les groupes terroristes qui privilégient désormais les méthodes asymétriques pour porter à l'adversaire, les coups les plus fatals. Désormais pour eux, tous les moyens sont bons dans l'atteinte des objectifs fixés. Par conséquent, eu égard à l'essor des technologies de l'information, ces groupes ont annexé l'univers des réseaux sociaux dont le contrôle échappe le plus souvent aux Etats.

C'est à ce titre que Fabrice Lollia[1] déclare: «Ils (les terroristes) utilisent d'ailleurs un vocabulaire issu des études stratégiques en expliquant que dans un conflit asymétrique traditionnel, l'état est avantagé par sa capacité à maîtriser les canaux de communication et de l'information. Mais, les nouvelles technologies de l'information brisent cette dynamique en permettant aux groupes terroristes de toucher le public par le biais de nombreux autres médias».

[1] Fabrice L., Terrorisme, Internet et Réseaux Sociaux, Février 2021.

Au regard de l'évolution actuelle des technologies de l'information, quelles réponses proposer pour faire face à l'omniprésence délictueuse des groupes terroristes et sécessionnistes dans les réseaux sociaux ?

En d'autres termes, alors qu'on assiste progressivement au basculement des groupes sécessionnistes vers le terrorisme, selon les dynamiques[2] et les stratégies[3] observées, il y a lieu de questionner la posture des Etats, de la population et des organismes non étatiques face à la montée en puissance des groupes adeptes de la violence dans le cyberespace. Quelle perception ont les acteurs étatiques et non étatiques sur les actions des terroristes et sécessionnistes sur les réseaux sociaux quand on sait que ces groupes extrémistes et nihilistes utilisent de plus en plus ces outils de communication à des fins militaires ?

Après avoir démontré que les réseaux sociaux sont un terreau fertile pour les groupes terroristes et sécessionnistes (I), notre étude se propose d'analyser la posture des masses populaires face à cette utilisation (II) et de relever les avancées enregistrées par les entités étatiques et non étatiques dans la prise en compte de la présence des terroristes dans les réseaux sociaux (III).

I - ANALYSE DES MODES D'ACTIONS DES GROUPES TERRORISTES ET SECESSIONNISTES SUR LES RESEAUX SOCIAUX.

Avec l'évolution de la menace terroriste dans le monde, plusieurs groupes sociaux qui s'opposent à l'ordre établi, ont choisi le terrorisme comme moyen d'expression pour se faire comprendre par leurs interlocuteurs généralement étatiques. D'où la similitude avérée entre groupe terroriste[4] et groupe sécessionniste[5]. Force est de constater que les

[2] Une dynamique est un changement, une évolution et, par extension, une capacité à changer, à évoluer. Elle peut être positive (croissance) ou négative (déclin).

[3] Les stratégies renvoient aux différents modes d'action d'un groupe, les procédés, les plans mis en œuvre pour atteindre un objectif à long terme.

[4] Un groupe terroriste est une entité qui emploie la terreur à des fins idéologiques, politiques ou religieuses. Certains groupes n'utilisent pas la violence mais ont un discours radical.

réseaux sociaux[6] sont la plateforme de cette analogie dans laquelle l'utilisateur[7] est généralement la cible.

A - DES SIMILITUDES AVÉRÉES

La propagande, le financement, l'entraînement, la planification, l'exécution permettent d'établir une similitude de modes d'actions entre les groupes terroristes et sécessionnistes sur les réseaux sociaux.

1 - LA PROPAGANDE, COMME TRONC COMMUN POUR LA PROMOTION DE LA HAINE

La propagande désigne un ensemble de techniques de persuasion, mises en œuvre pour propager une idée, une opinion, une idéologie ou une doctrine afin de pousser un public-cible à adopter une attitude donnée. Elle se caractérise, le plus souvent, par une influence médiatique, une création volontaire de la confusion, la manipulation de l'opinion publique, la falsification des images/ vidéos, la diffusion des informations partiales, les campagnes de diabolisation, etc.

Ainsi, elle est une forme de communication unidirectionnelle, qui prend parfois (mais pas toujours) la forme de la désinformation. Le recrutement, l'apologie et la radicalisation sont les principales manifestations de la propagande.

LE RECRUTEMENT

La portée des réseaux sociaux offre aux organisations terroristes et à leurs sympathisants un vivier mondial de recrues potentielles qui s'informent à travers les foras à accès restreint où sont poursuivis des objectifs bien définis. Les mineurs sont les principales recrues.

---

[5] Un groupe sécessionniste est une entité qui prône, au plan politique, la séparation volontaire d'une partie de la population d'un État, par voie pacifique ou violente, pour constituer un État indépendant ou pour se réunir à un autre.

[6] Les réseaux sociaux peuvent être définis comme des sites et applications web qui, reposant sur la technologie du web 2.0 et sur le principe d'expression, d'identification et de participation, permettent la création et l'échange des contenus générés par les utilisateurs identifiés par leurs comptes ou profils personnels accessibles totalement ou partiellement au public.

[7] Coutant A. et Stenger T. (2010). Processus identitaires et ordre de l'interaction sur les réseaux socio numériques. *Les Enjeux de l'Information et de la Communication*, 1, http://lesenjeux.u-grenoble3.fr/2010/Coutant-Stenger/index.html.

L'APOLOGIE

L'apologie de la haine, du crime ou du terrorisme peut consister, non seulement, en la présentation, le commentaire favorable, mais aussi la provocation, l'incitation directe, l'appel à la commission d'actes y afférents et matériellement déterminés, qui doivent être commis en direct sur un réseau social ouvert au public comme Facebook, Twitter, Instagram, WhatsApp, etc.

LA RADICALISATION

La radicalisation fait essentiellement référence à l'endoctrinement qui accompagne généralement la transformation de recrues en individus déterminés à commettre des actes de violence au nom d'idéologies extrémistes. Le processus de radicalisation implique souvent l'utilisation de la propagande, personnellement ou sur les réseaux sociaux, pendant un certain temps.

LES AUTRES MODES D'ACTIONS

Il s'agit du financement, de l'entraînement, de la planification et de l'exécution des attentats. Les organisations terroristes et leurs sympathisants ont parfois recours aux réseaux sociaux pour lever et collecter des fonds destinés au terrorisme. Ces transferts interviennent souvent par virement électronique, carte de crédit ou autres moyens de paiement disponibles. Une gamme variée de médias propose des plates-formes de diffusion de guides pratiques, présentés sous forme de manuels en ligne, de clips audio et vidéo, d'informations et de conseils, des instructions détaillées, faciles d'accès et en plusieurs langues, sur certaines méthodes, techniques ou connaissances opérationnelles (fabrication des explosifs, des armes à feu, matières dangereuses) etc. La capacité des réseaux sociaux à abolir les distances et les frontières, en font un outil essentiel pour planifier les actes terroristes. Les médias sociaux sont exploités par les organisations terroristes comme arme de recrutement et de propagande. C'est ce que l'on appelle «l'arsenalisation» des médias sociaux.

B - L' «ARSENALISATION» DES RÉSEAUX SOCIAUX PAR LES TERRORISTES

Certaines entités s'intéressent, de plus en plus, à l'usage qu'ils peuvent faire des médias sociaux contre leurs adversaires, un processus que Thomas Elkjer Nissen, du Royal Danish Defence College, appelle «l'arsenalisation» des médias sociaux. Dans ce cas, les réseaux sociaux peuvent être utilisés pour la collecte de renseignements, la guerre psychologique et même les activités de commandement et de contrôle (C2).

1 - LE CAS DE DAECH

Daech n'est pas la première organisation terroriste à comprendre l'importance des médias sociaux. Des membres du Hamas auraient utilisé des plateformes comme Facebook et Twitter pour diffuser leur idéologie.

UN MODUS OPERANDI TRÈS HUILÉ À TRAVERS TWITTER.

Il est communément admis que Daech a donné une nouvelle dimension à l'utilisation malveillante des médias sociaux. Ce groupe semble avoir compris comment utiliser ce qu'on appelle sur les réseaux sociaux, la «courbe de puissance». À une extrémité de la courbe, quelques contributeurs de premier plan dirigent la conversation sur le réseau («mode diffusion»). À l'autre extrémité, les réseaux mettent en relation de très petits groupes au sein desquels se déroule une conversation de haut niveau («mode conversation»)[8].

UNE PUISSANTE ARCHITECTURE D'INFLUENCE.

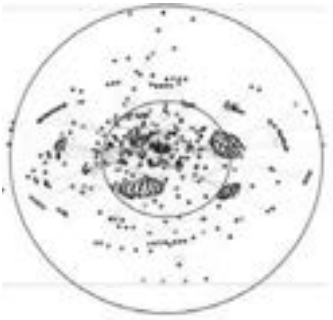
L'architecture de Twitter est parfaitement adaptée pour Daech car elle favorise les communications anonymes touchant un public très large et permet la récupération plus rapide de comptes désactivés[9].

---

[8] Carafano, J. J. *"Twitter Kills: How Online Networks Became a National-Security Threat*." TheHeritageFoundation, 8juin2015.http://www.heritage.org/defense/commentary/twitter-kills-how-online-networks-became-national-security-threat.

[9] Shaheen, J., Shaleen. "*Network of Terror: How Daech Uses Adaptive Social Networks to Spread Its Message*," Novembre 2015. http://stratcomcoe.org/network-terror-how-daesh-uses-adaptive- social-networks-spread-its-message.

Illustration d'une structure centre/périphérie



Cette figure est un exemple de l'un des réseaux de trafic recueillis, représenté à l'aide d'un cercle pour illustrer sa centralité. La technique de Daech centre-périphérie et une utilisation habile des hashtags assurent au groupe terroriste une forte visibilité sur les réseaux sociaux. Ainsi, alors que Daech entrait dans Mossoul, ses partisans ont envoyé jusqu'à 44 000 tweets par jour, faisant apparaitre le message du groupe en tête de liste lorsqu'on tapait «Bagdad» sur Twitter (Farwell).

UNE STRATÉGIE DE COMMUNICATION SAVAMMENT PENSÉE[10]

Le contenu de Daech est visuel (63 % d'images, 20 % de vidéos, 5 % de graphiques) (OTAN, COE Stratcom, 2016a), ce qui est particulièrement attrayant pour la jeune génération. Le contenu visuel est de qualité hautement professionnelle. Ce groupe terroriste tweete dans plusieurs langues dont l'anglais, l'arabe, l'allemand, le farsi, l'hindi et le français. Les messages de Daech sont en lien avec l'actualité, ils sont courts et faciles à comprendre. 16 % des comptes liés à Daech sont en fait automatisés («bots»).

2 - LE CAS DES GROUPES SÉCESSIONNISTES DU NORD-OUEST ET DU SUD-OUEST CAMEROUN

D'après un article du magazine Jeune Afrique[11], le contact dans les groupes sécessionnistes du Nord-ouest et du Sud-ouest est quotidien via WhatsApp ou Telegram, et les différents leaders y favorisent la coordination.

[10] Selon les estimations, plus de 30 000 personnes, dont environ 5 000 citoyens européens, se sont rendues en Syrie et en Irak pour grossir les rangs d'organisations terroristes depuis le début du conflit dans ces deux pays en 2011.
[11] Jeuneafrique.com/mag/715489/politique/crise-anglophone-au-cameroun-qui-sont-les-secessionnistes du …

UN NOUVEAU CADRE D'INFORMATION

Dans un article publié par Hans De Marie Heungoup Tanda Theophilus[12], le cas de la crise anglophone au Cameroun illustre parfaitement la mise en concurrence des médias classiques par les réseaux sociaux. Alors qu'un quotidien camerounais tire en moyenne 5000 exemplaires, les comptes Facebook des leaders des protestations au Cameroun sont suivis par des dizaines, voire une centaine de milliers de personnes. Le compte Facebook de Mark Bareta, une des figures du mouvement anglophone est suivi par plus de 130000 internautes.

UN LIEU DE RASSEMBLEMENT, DE SOCIALISATION POLITIQUE ET DE FORMATION À L'ACTION MILITANTE.

Les appels aux villes mortes et autres mots d'ordre de la contestation anglophone sont lancés via les réseaux sociaux. De fait, l'essentiel de l'architecture organisationnelle de la contestation est piloté via les réseaux sociaux. En avril 2017, Tapang Ivo Tanku, un des leaders anglophones, a émis plusieurs vidéos suivies par des dizaines de milliers de personnes. A travers ces vidéos, il appelait à la désobéissance civile et à la destruction des biens des agents de l'Etat. Le message de fin d'année 2017 du président autoproclamé de l'Ambazonie (République virtuelle anglophone) a été suivi sur les réseaux sociaux par plus de 100000 internautes, soit deux fois plus que celui du Président BIYA au même moment.

LES RÉSEAUX SOCIAUX COMME BALLON D'ESSAI

Les médias sociaux sont utilisés dans ce sens pour tester les opinions publiques sur des questions précises. Au début des grèves, les leaders de la crise anglophone s'en sont servis pour tester la légitimité de leurs causes auprès de la population. Sur Facebook, après chaque post sur les objectifs de la grève, les leaders ont souvent ajusté leur stratégie et message en tenant compte des milliers de commentaires de citoyens.

[12] Hans De Marie Heungoup Tanda Theophilus, Réseaux sociaux numériques et processus démocratiques en Afrique centrale: entre systèmes hégémoniques et nouveaux régimes de dissidence, Sep. 1, 2019 Publisher: Egmont Institute.

Plus largement, l'approbation des publications (posts)et mots d'ordre des leaders par les milliers de commentaires et mentions «j'aime»leur a servi de feu vert, au point que certains leaders comme Tapang Ivo, initialement fédéraliste et critiqué par les internautes pour cette position molle, ont rejoint le camp «ambazonien».[13]

LA SURINFORMATION

La surinformation est une stratégie qui permet de garder la cible concentrée sur un sujet précis, de semer la confusion entre vraies et fausses informations. Dans le milieu des activistes anglophones, plus d'une centaine d'entre eux publient des dizaines de posts par semaine sur la crise anglophone, dans le but d'inciter les populations à rejoindre le camp séparatiste. Ces activistes étant très suivis et leurs publications partagées, cela a contribué à entretenir la pression des réseaux sociaux sur le gouvernement camerounais.

LA DÉSINFORMATION ET LA PROPAGANDE

Au Cameroun, plusieurs fausses images et vidéos de tueries circulent depuis la crise dans les régions du Nord-ouest et du Sud-ouest, certaines ayant été prises dans des pays étrangers. De même, pour faciliter le boycott des cours par les élèves et le renforcement des «villes mortes», les grévistes anglophones ont, dès le début de la grève, fait croire à l'annulation de l'année scolaire et à la non-reconnaissance des diplômes de 2017 en zone anglophone par l'UNESCO. La publication d'anciennes images et vidéos des évènements ni géographiquement, ni même historiquement liées aux crises en question constitue un acte de désinformation et de propagande[14].

[13] L'Ambazonie (Ambazonia) est un terme utilisé par les séparatistes anglophones pour désigner l'État autoproclamé du Southern Cameroons.

[14] Au-delà des images et vidéos de torture vérifiées et vérifiables, plusieurs vidéos d'autres évènements ont surgi comme étant des vidéos et images des forces de sécurité torturant les populations.

II - POSTURES DES MASSES POPULAIRES FACE A L'UTILISATION DES RESEAUX SOCIAUX PAR LES GROUPES TERRORISTES ET SECESSIONNISTES

La montée en puissance des médias sociaux constitue l'une des manifestations les plus récentes et les plus importantes de la révolution numérique et des techniques de communication qui, il y a plusieurs décennies, a marqué le début de l'ère post-industrielle. La prolifération des médias sociaux ces dernières années a été facilitée par l'essor rapide des appareils mobiles connectés à Internet (smartphones). Selon une étude portant sur 50 000 jeunes de 26 pays, les médias sociaux supplantent déjà, pour cette génération, la télévision comme principale source d'information (Wakefield).

A - CIBLAGE DES JEUNES À TRAVERS LES RESEAUX SOCIAUX

Les masses populaires en général et les jeunes en particulier, constituent la cible privilégiée des groupes terroristes dans les réseaux sociaux. En effet, ils donnent le plus souvent aux jeunes, l'illusion de satisfaire tous leurs besoins fondamentaux.

1 - BESOIN D'UNE VISIBILITÉ IDENTITAIRE

Plusieurs jeunes fréquentent les réseaux sociaux parce qu'ils sont à la quête d'une affirmation de leur personnalité par une certaine identité individuelle ou collective qui peut envisagée sous l'angle de la mise en visibilité de soi, de l'expression d'une culture commune et de l'affichage des goûts et du capital social[15].Il s'agit d'une «exposition technologique de soi» par une «augmentation de l'autoproduction et de l'auto publication».

[15] Coutant A. et Stenger T. (2010). Processus identitaires et ordre de l'interaction sur les réseaux socio numériques. *Les Enjeux de l'Information et de la Communication*, 1, http://lesenjeux.u-grenoble3.fr/2010/Coutant-Stenger/index.html.

Ces médias deviennent ainsi des «scènes d'expression identitaire»[16], voire des «outils de reconstruction identitaire»[17].

2 - BESOIN D'EXPRESSION ET DE RENCONTRE

Les réseaux sociaux constituent des «catalyseurs relationnels»[18]. Les jeunes à travers les réseaux sociaux se font des relations (peu importe la nature) et communiquent avec autrui sans aucune gêne. Avec une identité numérique matérialisée par un «profil», ils peuvent échanger diverses informations avec d'autres correspondants. Les «manifestations du soi qui se jouent aux frontières de la pudeur et de l'intime, du privé et du public, du contrôle et du décontrôle, de l'intime et de l'estime à des fins de reconnaissance et de construction positive de son identité, dépendent des conventions implicites et/ou explicites qui en règlent la mise en pratique»[19].

Plus globalement, Coutant et Stenger dressent une typologie panoramique d'usages des réseaux sociaux chez les jeunes: retrouvailles entre amis, publication, partage et commentaire des photos, activités et événements, comparaison et évaluation de soi aux autres, jeux individuels et collectifs, messages instantanés, construction de son profil identitaire, édition des pages et groupes, et emails internes. À ces usages qui constituent l' «expression d'une culture juvénile»[20], trois enjeux majeurs sont liés notamment à l'identité, la sociabilité et la participation à l'action collective.

[16] Amri M. et Vacaflor N. (2010). Téléphone mobile et expression identitaire: Réflexions sur l'exposition technologique de soi parmi les jeunes. http://lesenjeux.u-grenoble3.fr/2010/Amri-Vacaflor/Amri-Vacaflor.pdf.
[17] Fluckiger C. (2010). Blogs et réseaux sociaux, outils de la construction identitaire adolescente ? *Diversité*, 162, p. 38-43.
[18] Granjon F. et Denouël J. (2010). Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux. *Sociologie*, 1(1), 25-43.
[19] Ibid.
[20] Dagnaud M. *Génération Y, les jeunes et les réseaux sociaux, de la dérision à la subversion*. 2011, Paris: Les presses de Sciences-po.

B - LES MASSES POPULAIRES VERS UNE RESILIENCE PROGRESSIVE

Face à la présence des terroristes sur les réseaux sociaux, l'on assiste comme à une prise de conscience progressive des masses populaires et à une construction des mesures d'autoprotection certes embryonnaires mais opportunes.

1 - UNE PRISE DE CONSCIENCE PROGRESSIVE

Face aux dangers et aux perversions présentes sur les réseaux sociaux, l'on assiste comme à une prise de conscience des masses populaires. En effet, eu égard aux diverses actions de sensibilisation menées par les organes étatiques sur la question des dangers sur les réseaux sociaux, les masses populaires semblent devenir prudentes sur les contenus des posts qu'elles reçoivent et surtout les sites à fréquenter.

Ces sensibilisations à but préventif ont porté, par exemple, sur l'usage des réseaux sociaux à des fins terroristes et la diffusion des informations personnelles. Cette prise de conscience progressive aboutit à une sorte de rejet.

2 - CONSTRUCTION DES MESURES D'AUTOPROTECTION

Afin de prévenir les dangers des réseaux sociaux, les internautes développent des mécanismes d'autoprotection en ligne, notamment par l'acquisition des logiciels qui permettent une protection des installations personnelles à un degré raisonnable contre les logiciels malveillants. Désormais des promoteurs d'anti-virus proposent des services qui permettent de bloquer les sites ou messages malveillants circulant dans les réseaux sociaux.

III - POSTURES DES STRUCTURES ETATIQUES ET NON ETATIQUES FACE A L'UTILISATION DES RESEAUX SOCIAUX PAR LES GROUPES TERRORISTES ET SECESSIONNISTES

Au fil des années, la stratégie d'isolement des groupes terroristes par les Etats et les entités dépositaires de l'usage réglementaire de la force est devenue obsolète avec les nouvelles technologies. En effet, il ne suffit plus de fermer les frontières pour réduire la mobilité des groupes terroristes, car avec les technologies de l'information, le message politique continue d'être diffusé auprès de la population[21]. Il est donc facile d'observer qu'internet permet aux groupes terroristes de s'assurer une présence virtuelle permanente qui facilite l'émergence de contenus numériques propices à l'organisation d'actions violentes[22].

A - POSSIBLES EVOLUTIONS ENREGISTRÉES

Au regard de l'avancée de l'hydre terroriste sur les réseaux terroristes, les Etats ont plus fait montre d'une attitude défensive, réagissant plus après coup, soit par la mise en œuvre de mécanismes juridiques répressifs ou par la création d'organismes de lutte et de veille. Ils ont été rejoints dans cette posture par les opérateurs des réseaux sociaux. Mais cette posture constamment défensive dénote surtout du manque de synergie entre les administrations en charge de la lutte contre l'expression du terrorisme et du sécessionnisme dans les réseaux sociaux.

1 - POSTURE PERMANEMMENT RÉACTIVE DES ETATS

En 2019, Mohamed Benabid relevait qu'au vu de la multiplication de pressions institutionnelles et réglementaires visant à lutter contre la haine en ligne, l'Assemblée Nationale Française a, en juillet 2019, voté la loi

[21] Kiras J.D. Irregular warfare: Terrorism and insurgency, 2007, Understanding modern warfare, 224,186□207.
[22] Torok R,2010, "Make A Bob in Your Mums Kitchen": Cyber Recruiting and Socialization of 'White Moors' and Home Grown Jihadists.

AVIA qui impose aux plateformes numériques de retirer un contenu en 24 heures. Aussi, les médias AFP, BFM TV, L'Express et Le Monde se sont associés à Facebook et à Google pour lancer de nouveaux outils de vérification des faits visant à venir à bout des fausses informations.

Au Royaume-Uni, il a été créé une Unité de lutte contre le terrorisme sur Internet (CTIRU) qui porte à l'attention des fournisseurs de services, les contenus qu'elle juge contraires à la législation antiterroriste nationale. Depuis sa mise en place en février 2010, la CTIRU a collaboré avec plus de 200 fournisseurs de services de télécommunications et a réussi à faire supprimer plus de 260 000 contenus de type terroriste.

Au Canada, le gouvernement estime que la collecte de données fiables et l'identification des meilleures pratiques internationales pour contrer les messages terroristes sont des éléments fondamentaux de sa stratégie de lutte contre le terrorisme. Le Réseau canadien pour la recherche sur le Terrorisme, la Sécurité et la Société (TSAS) a vu le jour en 2010 pour contribuer au corpus mondial de connaissances sur l'utilisation des médias sociaux par les terroristes et les stratégies pour la contrer.

Au Cameroun, la loi N°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité au Cameroun et la loi N°2014/28 du 23 décembre 2014 portant répression des actes terroristes sont des instruments répressifs pour lutter contre les déviances sur les réseaux sociaux. A ces deux textes s'ajoutent les actions de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC)[23]dans le domaine de la veille sécuritaire. A cette approche répressive s'intègre une approche pédagogique telle que voulu par S.E Monsieur Paul BIYA quand il déclare «*soyez des internautes patriotes qui œuvrent au développement et au rayonnement du Cameroun, non des followers passifs ou des relais naïfs des pourfendeurs de la République*»[24].

[23] ANTIC est un établissement public administratif doté d'une autonomie financière. Elle est créée par le décret présidentiel n°2002/092 du 8 avril 2002 modifié et complété par le décret n°2012/180 du 10 avril 2012 qui fixe l'organisation et son fonctionnement.

[24] Discours à la jeunesse le 10 février 2018 du Président du Cameroun, SE Monsieur Paul BIYA.

LES ACTIONS MENÉES DES OPÉRATEURS DES RÉSEAUX SOCIAUX

Au regard de l'évolution de la menace terroriste sur les réseaux sociaux, les principales entreprises des médias sociaux ont lancé plusieurs nouvelles initiatives pour combattre cette avancée. En Juin 2016, Facebook, Microsoft, Twitter et YouTube ont annoncé la création du Forum mondial de l'Internet contre le terrorisme, une plateforme de partage d'informations entre les géants de l'Internet, de sorte que les extrémistes violents ne soient plus accueillis par leurs services. En décembre 2016, ces opérateurs ont annoncé la création d'une base de données commune comprenant les empreintes numériques des contenus (images terroristes violentes, vidéos aux fins de recrutement terroriste et autres images qui seront retirées de leurs plateformes).

En avril 2017, Facebook a pris des mesures à l'encontre de 30 000 faux comptes en France, ou les a supprimés, dans les mois qui ont précédé l'élection présidentielle française. Twitter dit avoir supprimé 235 000 comptes faisant l'apologie du terrorisme au cours des six premiers mois de 2016.

Le navigateur Google Chrome a lancé une nouvelle extension appelée First Draft News Check, qui aide les utilisateurs à authentifier les images et les vidéos et permet de partager ses conclusions avec d'autres utilisateurs. Google collabore par ailleurs avec YouTube, dans le cadre d'un programme appelé Redirect Method, pour viser les recrues potentielles de Daech et, à terme, les dissuader de rejoindre le groupe[25].

B - ESQUISSE DE PROPOSITIONS DANS UNE APPROCHE GLOBALE

Le 08 janvier 2015, le Président de la République S.E Monsieur Paul BIYA déclarait dans son discours en réponse au Corps Diplomatique, je cite: «À menace globale, riposte globale» comme pour définir la politique qui doit guider la réponse face à la menace terroriste sans cesse évolutive.

[25] Au moyen de mots clés et de phrases que recherchent souvent les gens attirés par Daech, ce programme redirige les internautes vers des clips sur YouTube, en arabe et en anglais, qui montrent des témoignages d'anciens extrémistes, des imams dénonçant le fait que Daech est une perversion de l'islam, et des clips décrivant les dysfonctionnements du prétendu califat de Daech.

1 - PROMOTION DE LA COOPÉRATION POLICIÈRE AUX PLANS NATIONAL ET INTERNATIONAL

Renforcer la coopération inter-Etats semble la solution majeure pour faire face à la présence des terroristes sur les réseaux sociaux. Car aucun pays n'est capable de faire face seul à cette présence qui est affranchie de toute règle de territorialité. En effet, un terroriste peut influencer plusieurs followers en Afrique alors qu'il est en Europe etc. Les Etats sont donc appelés à coopérer afin de disposer de tous les moyens nécessaires pour traquer au maximum les terroristes sur les réseaux sociaux.

Certains organismes spécialisés comme INTERPOL peuvent être mis à contribution pour rechercher les terroristes sur les réseaux sociaux. Cette agence analyse l'utilisation que font les terroristes des plateformes de médias sociaux afin d'appuyer le travail d'identification et de détection mené dans le cadre des enquêtes antiterroristes nationales. Lors de l'enquête relative à l'attentat du London Bridge au Royaume-Uni en 2017, INTERPOL a aidé les enquêteurs à identifier d'éventuels témoins sur les médias sociaux, en utilisant la technologie de reconnaissance faciale.

2 - PROMOTION DE LA SYNERGIE ENTRE ADMINISTRATIONS EN CHARGE DE LA LUTTE CONTRE LE TERRORISME

A - ACTIONS CONCERTÉES

Face à l'évolution de la menace terroriste, les Etats sont généralement pris de cours par la célérité des actions terroristes, malgré diverses mesures prises. Le plus souvent les terroristes exploitent les faiblesses du système dont la plus criarde est le manque de collaboration entre différentes administrations poursuivant les mêmes buts, sinon connexes. Véritablement, pour venir à bout de la menace terroriste sur les réseaux sociaux, il faut une stratégie concertée entre différents départements ministériels au plan national. Cette stratégie peut se décliner sous forme de politique de lutte ou plan d'action national etc.

En mars 2018, le Gouvernement togolais décidait de renforcer le volet répressif de la réglementation contre les dérapages constatés dans l'utilisation des réseaux sociaux par une campagne de communication visant la mise en place de politiques d'éducation et de prévention pour faciliter la collecte du contenu illicite sur les réseaux sociaux.

B - PARTAGE DES INFORMATIONS AU NIVEAU NATIONAL.

L'«arsenalisation» des réseaux sociaux par les terroristes et les sécessionnistes a mis en exergue l'obsolescence des procédures des Services en charge du renseignement dans plusieurs pays, à cause de la maîtrise de l'outil informatique par les terroristes. En dehors de la réadaptation et du renforcement des procédures dans lesdits services, les administrations chargées du renseignement au niveau national devraient mettre l'accent sur le partage des informations surtout celles tirées des réseaux sociaux.

Le partage des informations est primordial pour venir à bout du cyber terrorisme dans les Etats, pour disposer de toutes élements de recherches nécessaires pour endiguer la menace. En Afrique, cette mesure est impérative au regard des difficultés financières que connaissent les Etats. La communauté de renseignements est un cadre institutionnel qui pourrait favoriser ces échanges et la mutualisation des moyens entre agences. A titre illustratif, en Côte d'Ivoire, la Communauté de Renseignement est un organe de veille de niveau stratégico-politique qui permet d'anticiper efficacement les menaces.

CONCLUSION

La thématique «l'utilisation des réseaux sociaux par les groupes terroristes et sécessionnistes: dynamique des acteurs» trouve ainsi toute sa pertinence car, elle plonge les analystes dans une problématique contemporaine qui consacre une certaine évolution de la conflictualité entre entités dépositaires de la force légale et terroriste (sécessionniste). A

l'observation des différentes pratiques des groupes terroristes et sécessionnistes dans les réseaux sociaux, l'on assiste à un emploi abusif de ces plateformes informatiques à des fins militaires, donnant l'impression d'une «Arsenalisation» de l'espace cybernétique.

Malheureusement pour le monde, alors que ces groupes prennent une avance fulgurante dans les réseaux sociaux, les masses populaires montrent une faible volonté à se protéger des dangers de cette omniprésence entretenue par des contenus attrayants qui attirent plusieurs jeunes d'où l'urgence d'une réponse adéquate des masses populaires.

Aussi, face à la montée de l'extrémisme, les Etats ont engagé des réformes au plan juridique par la promulgation de diverses lois pour réguler, voire contrôler l'usage des réseaux sociaux et sanctionner les éventuels délinquants. A leurs efforts se sont joints ceux des opérateurs de réseaux sociaux tels que Facebook, Whatsapp, Twitter, Instagram etc. Mais ces efforts semblent insuffisants car ils sont menés unilatéralement. Ces opérateurs ont mené des actions stratégiques contribuant à lutter contre la survenance des posts incitant au terrorisme et à sensibiliser les internautes sur l'indentification de ces contenus malveillants. Plusieurs comptes ont été supprimés dans divers pays dans le but d'assainir l'environnement des réseaux sociaux devenu un lieu d'épanouissement de la jeunesse. Les dynamiques et stratégies des différents acteurs sont évolutives. Elles sont issues de l'instauration des cadres privilégiant la collaboration et la synergie entre acteurs afin de disposer d'une solution globale qui permet d'explorer tous les contours du problème de la présence des groupes terroristes (sécessionnistes) sur les réseaux sociaux.

REFERENCES BIBLIOGRAPHIQUES

1 F. Lollia, Terrorisme, Internet et Réseaux Sociaux, Février 2021.

2 Coutant A. et Stenger T. (2010). Processus identitaires et ordre de l'interaction sur les réseaux socio numériques. Les Enjeux de l'Information et de la Communication, 1, http://lesenjeux.u-grenoble3.fr/2010/Coutant-Stenger/index.html.

3 Kiras, J.D. Irregular Warfare: Terrorism and insurgency, 2007, Understandingmodernwarfare, 224,186-207.

4 Torok, R, 2010, "Make A BombinYour Mums Kitchen":Cyber Recruiting and Socializa-

tion of`White Moors'and Home

5 Dagnaud M. *Génération Y, les jeunes et les réseaux sociaux, de la dérision à la subversion*. 2011, Paris: Les presses de Sciences-po.

6 Amri M. et Vacaflor N. (2010). Téléphone mobile et expression identitaire: Réflexions sur l'exposition technologique de soi parmi les jeunes. http://lesenjeux.u-grenoble3.fr/2010/Amri-Vacaflor/Amri-Vacaflor.pdf.

7 Fluckiger C. (2010). Blogs et réseaux sociaux, outils de la construction identitaire adolescente ? Diversité, 162, p. 38-43.

8 Granjon F. et Denouël J. (2010). Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux. Sociologie, 1(1), 25-43.

9 Jeuneafrique.com/mag/715489/politique/crise-anglophone-au-cameroun-qui-sont-les-secessionnistes du …

10 Hans De Marie Heungoup Tanda Theophilus, Réseaux sociaux numériques et processus démocratiques en Afrique centrale: entre systèmes hégémoniques et nouveaux régimes de dissidence, Sep. 1, 2019 Publisher: Egmont Institute.

11 Carafano, James Jay Carafano. Twitter Kills: How Online Networks Became a National-Security Threat." The Heritage Foundation, 8 juin 2015 .http://www.heritage.org/defense/commentary/twitter-kills-how-online-networks-became-national-security-threat.

LE ROLE ET L'INFLUENCE DES MEDIAS DANS LA PRESERVATION DE LA COMPETIVITE ECONOMIQUE DES ETATS

Wolfgang OWONA
Docteur, Diplomate, Expert en Sécurité Internationale et Chercheur, Formateur au Séminaire Afrique de l'Ecole Internationale de Guerre de Yaoundé

RESUME

L'absence de stratégie médias pour les Etats africains freine suffisamment leur capacité d'intégration dans la mondialisation et la possibilité pour ces derniers de maitriser la fourniture des contenus informationnels sur leurs pays afin de faire de celle-ci un instrument décisif dans la formulation des stratégies de compétitivité économique des Etats du Continent Noir. Pour ce faire, il importe pour ces derniers de formuler des stratégies d'attractivité économique à dimensions nationale, régionale et internationale, à destination des publics cibles nationaux, investisseurs extérieurs et des diasporas pour capter les niches de croissance et de doper leur compétitivité économique. Ces stratégies doivent être guidées par la recherche d'intérêts locaux et d'ouverture par la formulation des mécanismes susceptibles d'influencer de manière significative leurs marchés et leurs opinions nationales sur le plan interne et de se positionner en sources d'informations crédibles pour les potentiels investisseurs extérieurs.

Avec le boom du numérique dû à la globalisation qui fait entrer le

monde dans l'ère du digital roi et du règne de l'image[1], voire de l'hégémonie de son radicalisme et de sa puissance dans la fabrication des perceptions, du bien, du bon et du vrai, l'Afrique non sans difficulté[2], apparait comme un nouveau «territoire du numérique»[3]. Ce territoire qui porté par une jeunesse de plus en plus hi-tech, s'extasie dans les méandres et les dédales du cyberespace[4] avec des fortunes diverses, voit aussi celui des médias et des «espaces virtuels»[5] échapper au contrôle et à la maitrise des Etats africains, comme la technologie tout simplement avant lui. Ce qui apparait moins visible c'est que les médias, comme le cyberespace lui-même, constituent des espaces-enjeux[6], des espaces de compétition, voire des espaces de guerres nouvelles[7]. Il va sans dire qu'en observant, la phénoménologie médiatique et médiasphérique sur le Continent, force est de constater que la préférence et le choix assumés de la jeunesse et de l'opinion africaines qui pour s'informer, même sur des questions internes, préfèrent opter pour des solutions exogènes. Aussi, après avoir pris fait et cause quelques dizaines d'années avant, pour la télévision par câble et par satellite, portée par la figure symbolique et fortement expressive de l'antenne parabolique. Dans ce contexte: on constate que la défaite des nations et de l'opinion africaine sur la possession des médias, sur la capacité à «faire l'opinion» et sur la maitrise même de la promotion de l'image et des potentialités des Etats est une tendance attestée par la réalité. Si pendant longtemps la fracture numérique entre le reste du monde et l'Afrique était une tendance lourde, cette réduction s'observe de plus en plus au bénéfice

---

[1] Perez S. «9 - Le règne de l'image», Le Corps du roi. Incarner l'État de Philippe Auguste à Louis-Philippe, sous la direction de Perez Stanis. Perrin, 2018, pp. 213-232

[2] Bernard E., La transmission internet par satellite et l'Afrique: matérialité du système (Internet transmission by satellite and Africa: reality of the system). In: Bulletin de l'Association de géographes français, 78e année, 2001-1 (mars). Réseaux de télécommunications. Périurbanisation en Europe. pp. 17-25

[3] Beckouche P., «Chapitre 2. … une révolution économique ?», Les Nouveaux territoires du numérique. L'univers digital du sur-mesure de masse, sous la direction de Beckouche Pierre, Éditions Sciences Humaines, 2019, pp. 33-66

[4] Henri D, «Le cyberespace», Carnets de géographes [En ligne], 2 | 2011, mis en ligne le 02 mars 2011, consulté le 13 avril 2022.

[5] Margot B. et Henri D., «Espaces virtuels», Carnets de géographes [En ligne], 2 | 2011, mis en ligne le 02 mars 2011, consulté le 13 avril 2022

[6] Desforges A., «Les représentations du cyberespace: un outil géopolitique», Hérodote, vol. 152-153, no. 1-2, 2014, pp. 67-81.

[7] Douzet F. et Aude G., «Le cyberespace, ça sert, d'abord, à faire la guerre, Prolifération, sécurité et stabilité du cyberespace», Hérodote, vol. 177-178, no. 2-3, 2020, pp. 329-350.

du Continent[8], qui pour l'instant porte ses efforts telle une tendance positive irréversible. Pour l'agence Ecofin, on peut dire avec évidence que dans ce contexte: «on ne peut parler de développement sans parler de l'économie numérique. D'après Internet World Stats, le taux de pénétration d'Internet en Afrique s'élève au 30 juin 2019 à 39.8 %, soit 525 millions d'usagers, contre une moyenne mondiale de 57.3 %. Et selon le rapport GSMA 2018 sur l'économie numérique africaine, les technologies mobiles ont contribué à hauteur de 7.1 % du PIB de l'Afrique subsaharienne, soit 110 milliards de dollars»[9]. En opérant une analyse géopolitique des médias[10] en Afrique et dans le monde (voire figures), on peut constater que l'Afrique et le tiers-monde restent encore en retard [11] et contrôlent peu le marché médiatique et cybernétique africain. Cette réalité est davantage plus visible en Afrique subsaharienne où une industrie structurée et performante de l'économie des médias reste encore très peu envisageable, malgré des signaux prometteurs liés à l'avènement du numérique. Et pourtant, il s'observe paradoxalement une influence de plus en plus grandissante des médias sur la capacité à structurer les opinions et les gouts de consommation. D'ailleurs les plus radicaux diraient:»celui qui contrôle l'opinion, contrôle la consommation». Ce retard s'observe aussi dans le domaine des agences de notation[12], dont le rôle est déterminant dans le marketing-pays et la crédibilité financière de l'Etat, secteur où l'Afrique demeure encore peu visible, pourtant ces dernières structurent les logiques de perceptions des investisseurs sur les Etats et leur capacité à constituer des risques économiques et financiers viables et sûrs. Dans ce contexte Stanislas Zeze estimera qu' «on voit malheureusement certains pays qui se complaisent avec les notes données par *Standard* and *Poor's et Moody's*, parce que ce sont *Standard and Poor's et Moody's*. C'est dommage, il faut sortir de ce complexe, et se dire que

[8] Lire Sagna O., «La lutte contre la fracture numérique en Afrique: aller au-delà de l'accès aux infrastructures», Hermès, La Revue, vol. 45, no. 2, 2006, pp. 15-24.

[9] https://www.agenceecofin.com/industrie/2907-78980-grace-au-numerique-le-continent-africain-est-en-train-de-reduire-son-retard-par-rapport-aux-pays-developpes-huawei. Consulté le 15 avril 2022.

[10] Boulanger P., «Bibliographie», Géopolitique des médias. Acteurs, rivalités et conflits, sous la direction de Boulanger Philippe. Armand Colin, 2014, pp. 295-300.

[11] Barrat J., Géographie économique des médias, t. 1: «Médias et développement», t. 2: «Diversité des Tiers-Monde», Paris, Litec, 1992.

[12] Gaillard, N., «II. Définition, interprétation, typologie et modalités d'attribution des notations», Norbert Gaillard éd., Les agences de notation. La Découverte, 2010, pp. 16-42.

quand *S&P ou Moody's* vous donne un *B+*, cela veut dire «risque élevé». Il n'y a pas de quoi s'en réjouir»[13]. La compétitivité économique des Etats africains, instrument de souveraineté passe donc aussi par la capacité de ces derniers à développer des stratégies d'attractivité qui s'avèrent être des processus complexes,»longs et patients»[14].

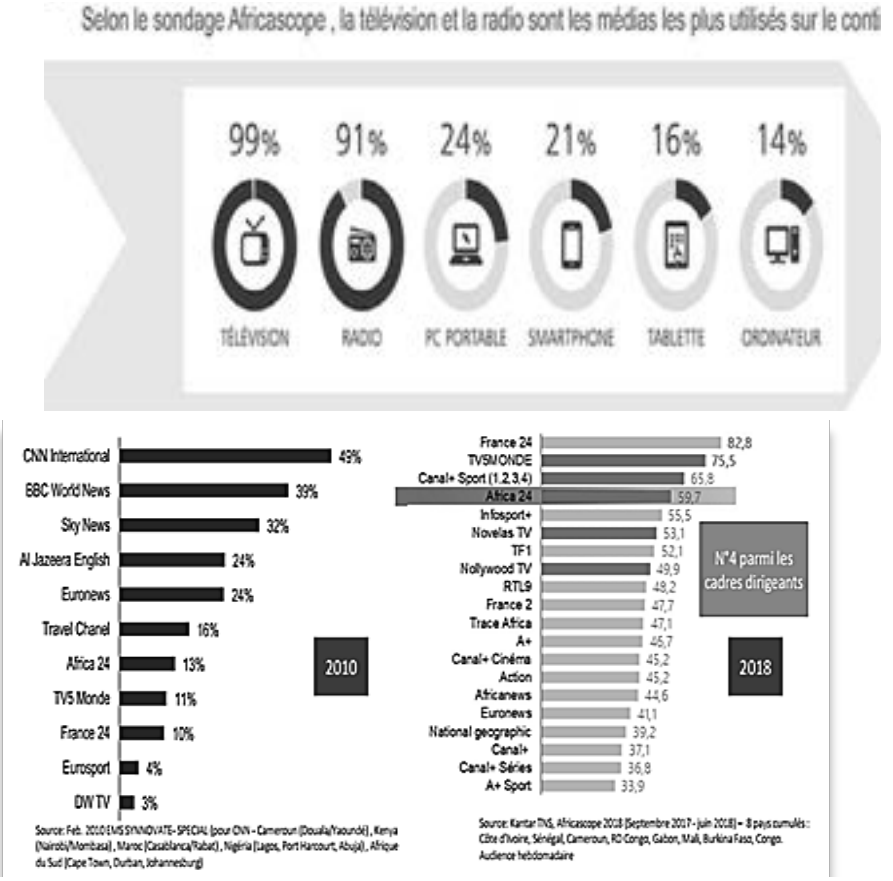
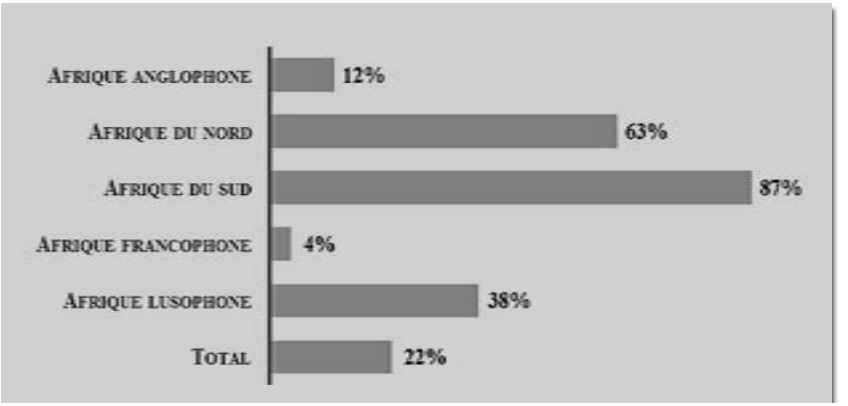


Figure 1: Les principaux médias [15] et chaines de télévision en Afrique [16]

[13] https://www.rfi.fr/fr/podcasts/afrique-%C3%A9conomie/20210906-les-agences-africaines-de-notation-financi%C3%A8re-commencent-%C3%A0-%C3%AAtre-prises-au-s%C3%A9rieux. Consulté le 13 avril 2022.
[14] Bourgain, A., Jean Brot, et Hubert Gérardin. «L'attractivité: quel levier pour le développement ?», Mondes en développement, vol. 149, no. 1, 2010, pp. 7-10.
[15] Africa24, Etudes: Audiences et donnes: 2020.
[16] Idem.



Figures 3 et 4: Les principales chaines panafricaines[17] et le Pourcentage d'intégration de l'Afrique sur le Marché mondial des programmes[18]

[17] https://www.telesatellite.com/actu/50279-le-top-10-des-chaines-les-plus-regardees-en-afrique-francophone.html
18

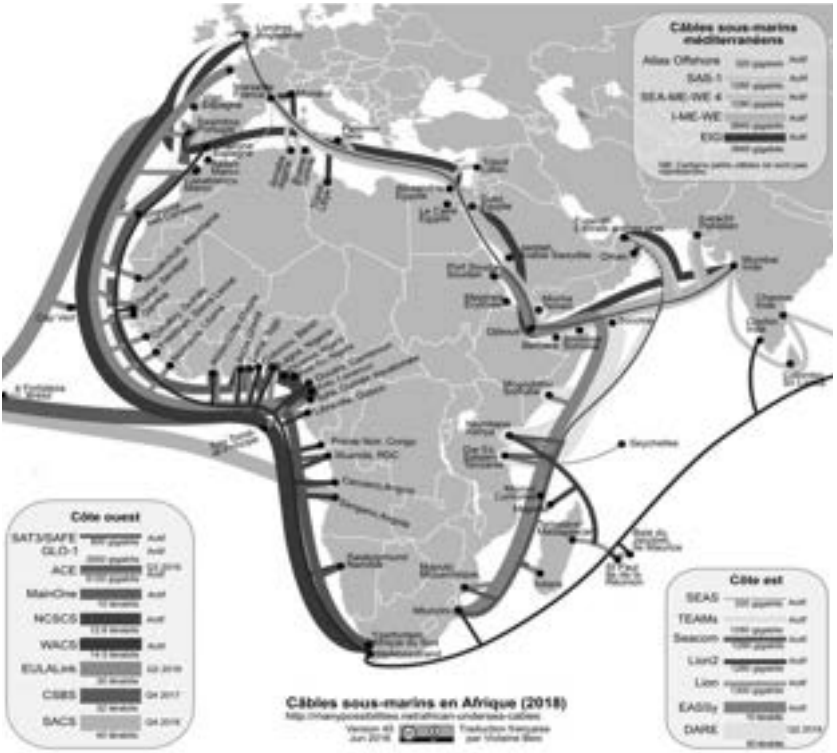


Figure 5: L'Afrique de l'Ouest dans le cyberespace: enjeux de sécurité et de souveraineté[19]

Par ailleurs, le développement du numérique avec l'infinité de possibilités et de corolaires qu'il offre, notamment par sa capacité à impulser et à doper la croissance socioéconomique en fait aussi un véritable enjeu de puissance économique[20], et de préservation de la souveraineté des Etats, notamment la souveraineté économique de ces derniers, comme élément constitutif important de la souveraineté nationale[21] dans un monde de plus en plus globalisé où la puissance et la vitalité économique font partie des critères de puissance et rayonnement des États. De plus, la quête et l'exercice de la puissance a souvent été perçue comme un leurre pour les Etats africains, voire une cause perdue, tant les facteurs structurels relèguent

[19] Méchinaud C., L'Afrique de l'Ouest dans le cyberespace: enjeux de sécurité et de souveraineté, Note d'Analyse du GRIP, 19 novembre 2019, Bruxelles.

[20] Muet P -A., «Impacts économiques de la révolution numérique», Revue économique, vol. 57, no. 3, 2006, pp. 347-375.

[21] Éric Chaplet, «La souveraineté économique au service de la souveraineté nationale:», Revue Défense Nationale, vol. N° 801, no 6, □ 1er juin 2017, p. 134–139

ces derniers à des positions d'acteurs marginaux de la globalisation, notamment dans la médiasphère mondiale, où ce sont précisément les *majors* globales qui imposent sans partage leur domination dans l'espace médiasphérique. Cette domination est d'ailleurs nourrie par la combinaison des moyens financiers et logistiques exorbitants, auxquels se greffe l'attractivité des programmes compétitifs soumis à la consommation cathodique des consommateurs. Au-delà de ces considérations, force est de constater que les référents sur le plan médiatique demeurent les *médias mainstream*[22], issus des principales puissances du directoire mondial, quand ce ne sont pas leurs agences de presses qui dictent le crédible, le non crédible, le viable et le non viable, voire gouvernent les perceptions du bon et du mauvais. Cette tendance se voit aussi au sein des agences de notation et diverses littératures spécialisées qui irradient de leurs sens et puissance la dynamique des perceptions économiques continentales, dans une absence plutôt remarquée des voies alternatives africaines fortes.

Si cette tendance est vraie dans une perspective de globalité, on peut aussi voir que dans les champs régionaux et sous régionaux d'Afrique, il émerge des espaces de compétition de la puissance symbolique qui constituent un élément à part entière de la puissance qui se veut une réalité globale et phénoménologiquement universelle[23]. La puissance, étant autant offensive que défensive[24], son acception dans cette perspective est spécifiquement défensive, en ce sens que le Continent, caractérisé dans sa contemporanéité par la modestie des facteurs de puissance, constitue un théâtre favorable, voire un banc d'essai pour ses propres médias dans l'ambition de contrer ceux venant irradier de leurs productions l'Afrique, dans leur ambition de «faire l'opinion»[25], de vendre l'image[26] des Etats Africains, voire d'en faire le «marketing-pays»[27] susceptibles de contrer les images souvent approximatives et peu conformes à la réalité. Cette préoccupation plurielle se trouve au cœur de la maitrise de cette

[22] Martel, Frédéric., Mainstream. Enquête sur la guerre globale de la culture et des médias. Flammarion, 2020

[23] Devin G., «II. La définition de la puissance», Guillaume Devin éd., *Sociologie des relations internationales*. La Découverte, 2013, pp. 29-36.

[24] Hoffmann S., «Raymond Aron et la théorie des relations internationales», Politique étrangère, vol. , no. 4, 2006, pp. 723-734.

[25] Champagne P., Faire l'opinion. Le nouveau jeu politique, Paris, Minuit, coll. «Le sens commun», 1990;

[26] Belaid Samy, «L'image du Pays. Proposition d'une échelle de mesure», La Revue des Sciences de Gestion, vol. 222, no. 6, 2006, pp. 141-147.

[27] Bomsel O., «Qu'est-ce que le numérique ?», Entreprises et histoire, vol. 43, no. 2, 2006, pp. 5-14.

communication, dans la finalité de booster la compétitivité et le rayonnement des Etats d'Afrique et de leurs collectivités locales[28]. Cette réflexion pose donc le besoin de l'utilisation stratégique de l'économie des médias et des nouveaux médias dans la préservation de la souveraineté des Etats africains, notamment de la souveraineté économique entendue ici comme l'état d'un système économique capable de «s'assurer de la disponibilité de certaines productions jugées essentielles.Autrement dit, celui de la compétitivité économie de l'industrie des médias d'Afrique sur le Continent. Comment rechercher la compétitivité et la souveraineté économique pour les Etats d'Afrique subsaharienne par la maitrise de l'économie des médias, tel est le kérygme de l'interrogation qui structure la dynamique de cette réflexion. Pour se faire, cette dynamique heuristique d'élucidation des pistes susceptibles de servir d'outils aux Etats d'Afrique subsaharienne procède par une articulation tripolaire dont la première mettra en lumière les fondements et enjeux de la maitrise des médias comme instruments de puissance (I), la seconde élucidera les divers théâtres d'instrumentation des médias par les Etats d'Afrique comme facteur de puissance (II), et dans la troisième articulation, il sera question de décliner les divers avantages que les Etats d'Afrique subsaharienne gagneraient à devenir «maitres et possesseurs»[29] d'une économie des médias performante, dans la perspective de préserver leur souveraineté économique (III).

I - LA COMMUNICATION COMME FACTEUR DE PUISSANCE DES ETATS: LES ENJEUX GEOPOLITIQUES ET GEOECONOMIQUES DE LA MAITRISE DES MEDIAS PAR LES ETATS AFRICAINS

La maitrise des représentations qui constituent un facteur de puissance important à l'aune de la mondialisation n'est plus à démontrer tellement leur influence dans les dynamiques géopolitiques et géoéconomiques des

[28] Rochette C., «Le marketing territorial: comment développer l'attractivité et l'hospitalité des territoires ? Chamard C. (sous la direction), Préface de Rousset A., avec la collaboration de Gayet J. et Alaux C., et la participation de Gollain V. et Boisvert Y. (2014), 203 pages, ISBN 978-2-8041-8472-8», Gestion et management public, vol. 6/1, no. 3, 2017, pp. 77-80.
[29] Descartes, Œuvres, éd. Adam/Tannery, t. vi, p. 62.

Etats sont visibles. De l'influence sur les investissements, et à celui la stabilité des marchés financiers, il est clairement observable que par l'action des médias, anciens et nouveaux, la tendance décrite se matérialise non seulement sur le plan interne, mais aussi sur le plan international. Vu sous cet angle, naviguer sans stratégie apparait comme une option de cécité, notamment pour les Etats d'Afrique subsaharienne ne jouissant pas de stratégies performantes visant à mobiliser ces instruments pour booster leur compétitivité économique. Face à cette situation, plus qu'une urgence, l'élaboration, et la construction des stratégies nationales d'emplois et de mobilisation des médias par les Etats subsahariens constituent une piste intéressante susceptible de leurs permettre d'avoir la maitrise des opinions émises sur et dans leurs propres pays d'une part, mais aussi sur l'évolution des dynamiques sociales et économiques qui structurent l'Afrique. Cette stratégie, une fois formulée, à l'image dun outil programmatique et doctrinal, pourrait emprunter deux principaux axes, dont le premier incombe aux gouvernements, et le second aux acteurs du secteur privé. Pour le gouvernement, il sera question de définir des cadres normatifs et économiques prenant en compte les exigences d'une structuration économique de l'industrie médiatique performante permettant aux Etats négro-africains de déployer leurs visions vers les diverses cibles posées en agents de consommation. Pour les seconds, il sera question de redoubler d'inventivité à l'effet de profiter de ce secteur dans le sens d'en créer de la valeur ajoutée dont les bénéfices profiteraient autant aux entrepreneurs, qu'aux Etats et nations africaines. Comme instrument, une telle stratégie devrait s'articuler sur des nécessités endogènes (1) et des fondements exogènes (2).

A - LES FONDEMENTS ENDOGÈNES DE LA MOBILISATION STRATÉGIQUE DES MÉDIAS COMME FACTEURS DE PUISSANCE

L'enjeu de la maitrise de l'opinion a toujours été présent dans les pays africains, et a toujours constitué un intérêt déterminant pour les Etats d'Afrique Noire. Pour s'en convaincre, on peut observer que dans tous les

pays d'Afrique subsaharienne, les gouvernements ont toujours misé sur la création et mise sur pied des chaines de télévision à capitaux publics contrôlées majoritairement ou entièrement par l'Etat, voire des organes de presses et des régies publiques de communication et de marketing. Du Cameroun au Nigeria en passant par la Zambie et l'Afrique du Sud, les gouvernements ont fourni des efforts à l'effet de mettre sur pied des instruments tels que la CRTV[30], la Société de Presse et d'Éditions du Cameroun SOPECAM[31], la *Nigerian Television Authority* (NTA)[32], la Zambia National Broadcasting Corporation (ZNBC), ou encore la *South African Broadcasting Corporation* qui pendant longtemps fut la caisse de résonnance du Parti national (*Nasionale party*), principale promotrice de l'apartheid. Ce qu'on peut constater, c'est que cette domination des médias publics dans le paysage médiasphérique avait principalement pour but de maitriser l'opinion à des fins de domination politique, sans y avoir la volonté de transformer ces derniers en véritables instruments et outils économiques, voire et géoéconomiques. Cette transformation en outils géoéconomiques qui vise principalement à faire de ces derniers de véritables instruments de la promotion des potentialités socioéconomiques nationales au service de la croissance et de la résilience face aux divers crises économiques ayant fait le lit des politiques d'ajustement structurel et d'approfondissement de la vassalisation économique des Etats africains, surtout ceux de l'Afrique subsaharienne francophone ne détenant pas dans leur politique économique l'instrument de souveraineté monétaire[33]. Cependant la mobilisation stratégique des médias comme facteurs de puissance sur le plan intérieur en Afrique à l'effet de concurrencer les autres médias extérieurs est possible. Elle est un intérêt à la portée des Etats africains. Pour y parvenir, il incombe d'abord aux gouvernements d'élaborer des cadres stratégiques de régulation qui tiennent compte de la vision et des intérêts nationaux préalablement définis et clarifiés. Dans cette perspective trois principaux instruments apparaissent adéquats: favoriser l'aide à la structuration du secteur de

[30] Office de radiotélévision à capitaux publics du Cameroun

[31] La Société de Presse et d'Éditions du Cameroun édite plusieurs titres de journaux à capitaux publics proches du gouvernement camerounais parmi lesquels on peut citer: *Cameroon Tribune*, Weekend *Sports* et Loisirs, *Nyanga*, et *Cameroon Business Today*.

[32] Le *Nigerian Television Authority* est le groupe audiovisuel public de la République Fédérale du Nigeria.

[33] Il s'agit principalement des Etats de la *zone franc* d'Afrique de l'Ouest et du Centre.

l'économie médiatique, faire un usage adéquat des leviers fiscaux dans ce secteur, et soutenir la prise de participation publique dans le capital des dites entreprises de communication.

Si la création des entreprises reste risquée[34], c'est aussi parce qu'elle charrie des difficultés à franchir, parmi lesquelles celles relatives aux formalités administratives liées à leur structuration. Cette réalité est encore plus perceptible en Afrique où le taux de scolarisation est bas, et la rareté des spécialistes est fortement ressentie par les promoteurs d'entreprises qui parfois ne jouissent pas des ressources techniques. Ici, on constate que de manière générale les profils d'entrepreneurs les plus récurrents sont ceux d›un: «autodidacte, parfois diplômé de l'enseignement supérieur, tour à tour jeune créateur sans expérience, cadre démissionnaire d'un grand groupe ou bien héritier d'une vieille affaire familiale»[35]. Dans l'industrie et l'économie des médias, on observe aussi de nombreux praticiens ayant décidé de se mettre à leur compte. Cette situation qui fait le nid de l'informel se vérifie dans plusieurs pays subsahariens. A titre illustratif, on peut citer le Cameroun où sur plus d'une dizaine d'opérateurs télé, aucun ne dispose d'une licence en bonne et due forme et fonctionnent dans un régime de «tolérance administrative»[36]. De plus il est difficile, malgré ce régime de tolérance administrative de voir ces médias orientés dans la recherche du rayonnement socioéconomique de leurs Etats par la promotion de leur potentialité socioéconomique, une prescription qui pourtant pourrait leurs être faite en compensation de cette situation de normativité déficitaire qui est la leur.

Atteindre cet état des choses passe nécessairement par la combinaison de plusieurs facteurs relevant de plusieurs sous-secteurs parmi lesquels on peut citer l'élaboration d'un modèle économique adéquat ayant comme objectifs stratégiques une gestion maitrisée des exigences liées à la formalisation administrative, au renforcement continue de l'audiométrie, en passant par le développement des programmes plus attrayants, et les prises importantes de

[34] Roux D., «La création des entreprises», Dominique Roux éd., Les 100 mots de la gestion. Presses Universitaires de France, 2011, pp. 7-15.

[35] Ben Hamadi, Zouhour, P Chapellier, et F Villesèque-Dubus, «Innovations budgétaires en PME: l'influence du secteur d'activité et du profil du dirigeant», Innovations, vol. 43, no. 1, 2014, pp. 223-252.

[36] Attitude des pouvoirs publics camerounais qui restent peu regardantes sur les exigences administratives requises pour certains usages socioéconomiques régies par la loi et la règlementation.

marchés. Dans cette optique, les médias africains gagneraient d'abord à se positionner comme des acteurs incontournables de la structuration de l'opinion et des habitudes de consommation sur le plan intérieur. Comme exigence de base de toute réussite entrepreneuriale, se trouve la capacité pour tout créateur d'entreprise de définir un modèle économique susceptible de permettre à son entreprise de de remplir ses fonctions, d'atteindre ses objectifs et d'engranger des bénéfices. Selon la nature et les spécificités du marché local, un modèle économique vise principalement à décrire «les principes selon lesquels une organisation crée, délivre et capture de la valeur»[37]. Pour ces défis de positionnement comme acteur crédible de la structuration des opinions, les médias d'Afrique doivent réussir à définir un modèle économique performant capable de leurs permettre de maitriser le marché intérieur de la publicité, de la communication et du marketing. A ces fondements endogènes, on peut évoquer quelques fondements exogènes.

1 - LES FONDEMENTS EXOGÈNES DE LA MOBILISATION STRATÉGIQUE DES MÉDIAS COMME FACTEUR DE PUISSANCE

L'influence du marché interne de la communication, de la publicité et du marketing-pays et celui des territoires n'est pas le seul lieu d'expression de la mobilisation de la puissance médiatique à des fins économiques. En faisant sien l'objectif de définir et d'élaborer sa stratégie de projection médiatique sur le plan externe, l'Etat négro-africain construit ainsi un instrument de sa puissance économique par sa capacité à influer sur les représentations qu'ont les investisseurs extérieurs sur son économie et ses potentialités. Dans cette optique, il devient dès lors important de définir les mécanismes susceptibles de doper l'attractivité du pays et de ses potentialités, en créant un contrepoids important face à la détérioration de l'image des pays africains à l'extérieur. Cela revient à construire l'image du pays, qui pourrait s'entendre comme l'ensemble des représentations mélioratives formulées visant à mettre en avant les potentialités politiques, «le degré de développement économique,

[37] Gallic C. et Marrone R., «Chapitre 2. Les modèles économiques», Le grand livre du marketing digital. Sous la direction de Gallic Claire, Marrone Rémy. Dunod, 2020, pp. 27-43.

le degré de développement technologique, la dimension culturelle»[38]. Cette démarche, dont l'objectif est d'«attirer des investissements sur un territoire, qu'il s'agisse d'un pays, d'une région ou d'une ville, est une activité complexe qui exige le développement d'une véritable méthode de la part des administrations publiques en charge de cette «promotion économique»[39] de l'Etat. Autrement dit, cette nécessité de définir une politique d'internationalisation des médias nationaux comme vecteurs de projection de l'image positive de l'Etat, passe aussi par un accompagnement institutionnel et diplomatique des gouvernements au bénéfice de leurs industries médiatiques à l'extérieur, dans le cadre de l'accompagnement aux entreprises privées, et des «cadeaux fiscaux»[40] conformes aux diverses législations nationales. L'implémentation d'une telle stratégie pourrait aussi passer par des prises de participation dans le capital de ces médias: corolaire à la capacité de prise de décision aux seins des conseils d'administration, et de la possession des capacités de blocage et d'orientation des entreprises. Ces différentes garanties permettraient aux gouvernements d'influencer les contenus des ces diverses chaines privées, à défaut d'avoir des chaines à capitaux publiques performantes disponibles dans les divers bouquets préalablement choisis sur leur capacité d'influencer les cibles de la politique d'attractivité nationale par les médias. Cette stratégie de projection des médias nationaux pourrait s'exercer dans des théâtres bien définis à la portée de la projection des Etats subsahariens.

II - LES THEATRES D'EXPRESSION DE L'INSTRUMENT MEDIATIQUE COMME FACTEUR DE PUISSANCE

Le renforcement de l'attractivité économique d'un Etat, entendue comme une la mise en avant d'un ensemble de facteurs économiques comme les ressources, «l'intégration économique, la qualification de la

[38] Belaid Samy, «L'image du Pays. Proposition d'une échelle de mesure», La Revue des Sciences de Gestion, vol. 222, no. 6, 2006, pp. 141-147.

[39] Lecat B., «Comment promouvoir son pays, sa région ou sa ville auprès des investisseurs étrangers ? Identification des critères d'implantation et de leur importance par l'entremise du marketing public», Reflets et perspectives de la vie économique, vol. xlvii, no. 2, 2008, pp. 71-83.

[40] Chartoire R., «Analyser les niches fiscales», Idées économiques et sociales, vol. 166, no. 4, 2011, pp. 39-47.

main-d'œuvre, la présence d'entreprises complémentaires, la qualité des biens et des services publics, des institutions, des règlementations…»[41], passent toujours par le développement d'une stratégie de marketing-pays forte et offensive à destination des cibles bien précises. En réalité, la référence au concept géostratégique de théâtre apparait adéquate pour exprimer le champ de projection et d'expression de toute politique d'influence médiatique visant à influencer et à structurer les opinions dans un espace donné[42], en l'occurrence un Etat ou une de ses régions. Dans le cas d'espèce, les théâtres susceptibles de constituer des enjeux de contrôle et/ou d'influence pour les Etats africains sont connus. En vertu des configurations spatiales, géoéconomiques et géopolitiques des Etats africains, quelques théâtres d'expression des stratégies de projection de la puissance médiatique au service du rayonnement économique des Etats Africains peuvent se décliner. Compte tenu de leurs ressources réduites des prétentions modestes susceptibles d'être les leurs, deux théâtres d'expression précisconstituent des objectifs à la portée des Etats Africains, ce sont les théâtres domestiques (1) et certains théâtres extérieurs (2).

1 - LES THÉÂTRES DOMESTIQUES COMME ESPACES DE PROJECTION DE LA PUISSANCE MÉDIATIQUE DES ETATS SUBSAHARIENS

A l'observation et à l'analyse, on constate que du point de vue de la médiamétrie et de l'audimétrie, les référents de littératures économique et d'information les plus prisés sont soit exogènes à l'Afrique, soit extérieurs au pays dont les consommateurs raffolent. Des dévots de TV5 Monde, en Passant par CNN et France 24, BBC, CBS, Chinua, VOA… l'Afrique consomme peu d'information économique issue de ses propres cénacles médiatiques, intellectuels et professionnels. Par ailleurs, très peu de chaines africaines essaient de faire le poids. Si le Nigéria se distingue sur le plan de la production des contenus culturels avec les chaines relayant le génie cinématographique de Nollywood, force est de constater que sur le plan de l'Information et de la promotion de l'image économique du Nigeria et de

[41] Bourgain A rnaud Jean Brot et Hubert Gérardin, «L'attractivité: quel levier pour le développement ?», Mondes en développement, vol. 149, no. 1, 2010, pp. 7-10.
[42] Lire Sourbès-Verger I., «Espace et géopolitique», L'Information géographique, vol. 74, no. 2, 2010, pp. 10-35.

ses potentialités, le pays a du mal à produire des mastodontes. Quant à l'Afrique du Sud, elle apparait comme une exception où les chaines nationales structurent l'opinion au niveau national où la *South African Broadcasting Corporation, la Revue sud-africaine* et ses sous titres *Mines, finances, commerce»* détiennent les principales parts de marché et donc les capacités à structurer l'opinion générale et spécialisée sur les questions économiques en Afrique du Sud sont certaines. Pour contrôler les théâtres domestiques, les Etats pourraient mobiliser les fonctions régulatrices qu'ils détiennent. Concrètement, il revient aux gouvernements mettre sur pied des mécanismes favorisant la création et le fonctionnement harmonieux des médias. Dans cette perspective, renforcer le tissu national de l'industrie médiatique comme une industrie à part entière[43] au service de l'attractivité économique de l'Etat apparait comme une piste intéressante. En plus de ce théâtre national de l'influence de l'opinion, on peut aussi évoquer les théâtres extérieurs.

2 - LES THÉÂTRES EXTÉRIEURS COMME ENJEU DE PROJECTION DE LA PUISSANCE MÉDIATIQUE DES ETATS AFRICAINS

La crédibilité comme le recours à un média sont toujours facteurs de son sérieux et de sa capacité à attirer des auditeurs, lecteurs et clients qui constituent les consommateurs des divers produits de la communication mis sur le marché. L'ensemble de ces atouts participent du renforcement de la qualité du produit délivré, susceptible d'être consommé hors des frontières de l'Etat et de permettre de se positionner en sources crédibles pour les publics cibles régionaux, voire, des diasporas. Cette réalité qui traduit une option d'internationalisation régionale, déjà observables chez les entreprises maghrébine[44], nigérianes et sudafricaines, mais encore peu visibles dans les autres pays négro-africains, qu'ils soient francophones ou anglophones, notamment dans le secteur de l'économie des médias et de la communication. Si de manière évidente la subsidiarité des entreprises africaines de communications leur donne un avantage susceptible d'être mobilisé dans leurs

[43] Sonnac N., «Les médias: une industrie à part entière et entièrement à part», Questions de communication, vol. 9, no. 1, 2006, pp. 455-473.

[44] El Qour, T., Belfahmi, B., «L'internationalisation des entreprises publiques comme outil d'intégration africaine: le biais de la diplomatie économique. Analyse de cas marocains», Revue «Repères et Perspectives Economiques» [En ligne], Vol. 4, Numéro spécial / novembre 2020, mis en ligne le 26 novembre 2020.

stratégies d'internationalisation, il n'en demeure pas moins vrai qu'au réalisant des études dans l'optique de «de réduire la part de hasard dans le processus du marketing»[45], les entreprises médiatiques publiques comme privées des Etats africains pourraient faire des projections aux niveaux régionaux limitrophes et des diasporas globales comme étant des publics-cibles de choix pour leurs intérêts . Dans cette perspective, deux solutions opératoires peuvent être implémentées. La première consisterait à soutenir quelques médias privés ayant déjà un fort potentiel d'internationalisation. Ici le Cameroun pourrait soutenir une stratégie d'internationalisation des médias nationaux tels *Africa24*, ou encore *Voxafrica* dans la sous-région Afrique Centrale, et le Golfe de Guinée pour booster son attractivité socioéconomique. Ou encore le Mali, face la conjoncture socioéconomique et sécuritaire, soutenir des chaines de de télévision tel *Africable*. La seconde consisterait à orienter la stratégie d'internationalisation des médias publics nationaux en favorisant leur insertion à court et moyen termes dans les grands consortiums de distributions internationaux ayant pour cibles leurs diasporas et les autres niches d'investisseurs internationaux. Dans un tel travail, les missions diplomatiques pourraient être mise à contribution a travers des structures dédiées à cet effet, et lesdits médias acheter des espaces de vulgarisation à l'effet de se vendre, et combattre ainsi l'image d'une Afrique donnée pas les autres acteurs sur elle-même. Aussi il ne serait pas superflu de soutenir la création d'agences de vulgarisation de l'information économique propres. Voilà pourquoi dans un contexte de quasi-absence des Etats Africains dans le marché de la notation financière au niveau mondial et même continentale, les créations de *Global Credit Rating*, *Bloomfield Investment*[46], et *l'African Global Rating*[47] sont à saluer, car elles constituent des alternatives sérieuses en termes de vulgarisation de notations financières des Etats Africains par les africains. L'implémentation et l'encouragement de tels mesures pourraient constituer des pistes d'intelligence économique de la part des Etats africains qui adopteraient ainsi des comportements rationnels dans l'optique de mobiliser l'économie des médias comme instrument de compétitivité économique, et par le fait même de souveraineté, en développant des stratégies d'influence sur les investisseurs et sur leurs diasporas au service de plusieurs avantages.

---

[45] **Dosquet F**., «Chapitre 1. Les missions des études de marché», Frédéric Dosquet éd., Études de marché. Dunod, 2018, pp. 1-35.

[46] *Bloomfield Investment* est la toute 1ère Agence de Notation Financière d'Afrique Francophone situé en Cote d'Ivoire. Elle fut créée en 2007.

[47] https://www.sikafinance.com/marches/l-ua-va-creer-sa-propre-agence-de-notation-financiere_33700. Consulté le 12 avril 2022.

III - LES AVANTAGES GEOECONOMIQUES DE LA MAITRISE DE L'ECONOMIE DE LA COMMUNICATION

La construction d'une stratégie d'influence médiatique par les Etats d'Afrique noire vise bien entendu des intérêts de natures pluriels. En ambitionnant comme configuration d'exercice des enjeux de types nationaux, mais aussi de types régionaux, l'implémentation d'une telle stratégie, dans une logique de puissance défensive, permettrait aux Etats africains d'atteindre des intérêts géoéconomiques et géopolitiques. Ces intérêts qui recherchés en interne (1), permettraient aussi de capter des niches d'intérêt exogènes au-delà de leurs frontières (2).

1 - LES AVANTAGES GÉOPOLITIQUES ET GÉOÉCONOMIQUES D'UNE ÉCONOMIE NATIONALE DES MÉDIAS VIGOUREUSE SUR LE PLAN INTÉRIEUR;

Les bénéfices susceptibles d'être engrangés par les Etats à travers la formulation et l'implémentation des stratégies nationales de médias, et de l'économie de la communication sont envisageables sur le plan domestique. Ils peuvent s'observer non seulement sur le plan strictement géopolitique, mais aussi dans une perspective géoéconomique. Sur le plan de la géopolitique interne, deux motivations peuvent justifier à suffisance le développement de stratégies médias, et de stratégies de communication à l'échelle étatique. Ce sont la nécessité de contrer les mécanismes de désinformation hostiles à la politique intérieure des Etats d'une part, et la nécessité de disposer des relais sûrs d'information susceptibles d'être mobilisés en cas de besoin d'autre part qui en justifient la pertinence. En satisfaisant à la première exigence, l'Etat réussit à disposer d'instruments lui permettant de maitriser le moral des populations face au développement important des *fakes news*, accentué par la mondialisation et la digitalisation de plus en plus importante dont les sociétés africaines acceptent. Ces dernières se situant au carrefour des croyances et de la manipulation en tant qu'interactions sociales et communicationnelles transactionnelles et

circulaires»[48], avec une rupture insidieuse du contrat narratif[49], préalable dans tout acte de communication entre les émetteurs et les récepteurs.

Dans la nécessité de disposer des relais sûrs d'information, il apparait clair qu'elle relève davantage du renforcement des mécanismes de loyauté des entrepreneurs médiatiques au services du rayonnement politique et économique de l'Etat, de la promotion de son image et de ses potentialités à destination d'un public cible à l'échelle nationale. Ici l'enjeu est davantage d'orienter les acteurs économiques vers les sources d'informations nationales sur les potentialités et les opportunités économiques dont regorge chaque Etat. Si l'option prise par certains gouvernements africains est de soutenir des hommes d'affaires solitaires sans mécanisme plus solides et structurés tels que des prises de participation, et de contrôle des parcelles de pouvoir au sein des dites entreprises, force est de constater que l'arme fiscale qui bien que constituant un instrument de politique économique pour l'Etat, qui en use et en abuse parfois d'une manière plus ou moins opportune»[50], demeure peu efficace et participe d'avantage d'une démarche autoritaire. Cette consolidation des intérêts géopolitiques des Etats consacrerait aussi des avantages géoéconomiques pertinents.

Sur le plan macroéconomique, le développement de stratégies médias et de communication par les Etats africains dans l'optique de doper leur compétitivité économique induirait à des progrès indéniables. Comme instruments d'orientation et de structuration de politiques publiques, les stratégies procèdent aussi par des mécanismes visant à formaliser leurs champs d'applications, et l'économie des médias en fait pas partie. De manière générale, il est important de préciser que les médias qu'ils soient publics ou privés, constituent des entreprises à part entière. Il apparait donc clair que «les journaux, stations de radio et de télévision, sites d'information ne constituent pas seulement des entités qui contribuent au débat politique et incarnent la démocratie: ils reposent sur des appareils de production qui positionnent leur produit dans un marché concurrentiel, où s'imposent les

[48] Giry J., Les fakes news comme concept de sciences sociales. Essai de cadrage à partir de notions connexes: rumeurs, théories du complot, propagande et désinformation», Questions de communication, vol. 38, no. 2, 2020, pp. 371-394.
[49] Mathieu-Castellani G., «Devis/récits: le cadre et le contrat narratif», La conversation conteuse. Les nouvelles de Marguerite de Navarre, sous la direction de Mathieu-Castellani Gisèle. Presses Universitaires de France, 1992, pp. 57-78.
[50] Rossignol J -L., «Fiscalité et responsabilité globale de l'entreprise», Management & Avenir, vol. 33, no. 3, 2010, pp. 175-186.

impératifs de survie de l'entreprise»[51] se caractérisent par un niveau élevé d'informel. Cette réalité est fortement visible au Cameroun[52], comme dans d'autres pays africains (Mali, Cote d'Ivoire, Nigeria…). Sans pour autant postuler un niveau zéro de formalisation, le déficit de formalisation est important, et la construction des stratégies nationales médias apparaissent comme des vecteurs importants de formalisation de ce secteur économique hautement stratégique. Au delà de cette formalisation économique dans un secteur fortement marqué par le caractère informel des structures de production de l'économie de la communication et des médias, on peut aussi évoquer une augmentation quantitative.

Les mutations survenues par le truchement du cyberespace dans l'économie de manière générale, et dans le secteur de l'économie numérique en particulier impactent aussi l'économie de la communication en suscitant un engouement important pour la création des entreprises de communication travaillant essentiellement dans le numérique. Ces bouleversements significatifs des modalités de consommation, de fonctionnement et de production des biens[53] favorisés par l'avènement et la vulgarisation d'internet incite les entrepreneurs à éprouver leurs génies par une création de plus en plus importante d'entreprises[54] et de médias. L'inflation observée des officines communicantes qui constituent des niches de vulgarisation de l'attractivité économique de l'Etat, traduit sur le plan quantitatif une avancée indéniable. C'est dans cette perspective que pour la ministre camerounaise des Postes et Télécommunications: «faut un écosystème particulier pour les multiples millions de jeunes camerounais compétents, dynamiques pour pouvoir s'exprimer et propulser le Cameroun véritablement vers l'émergence numérique»[55], au service de la réduction du chômage. L'inflation des *starts up,* des activistes cybernétiques et la multiplication des AGR[56] dans le domaine de la communication via le

[51] Frère M -S., «Chapitre 6. L'économie des médias en Afrique francophone», Journalismes d'Afrique. Sous la direction de Frère Marie-Soleil. De Boeck Supérieur, 2020, pp. 259-300.

[52] Lire Atenga T., Madiba G., La communication au Cameroun: les objets, les pratiques, Paris, Archives Contemporaines Editions, 2012, 180 p.

[53] Sonnac N. et J. Gabszewicz, «IV. Marchés et stratégies des médias à l'ère numérique», Nathalie Sonnac éd., L'industrie des médias à l'ère numérique. La Découverte, 2013, pp. 57-84.

[54] A. F. Loukou, «Les TIC au service du développement en Afrique», tic&société Vol. 5, n°2-3 | 2e sem. 2011 / 1er sem. 2012, avril 2019.

[55] https://www.minpostel.gov.cm/index.php/fr/actualites/407-economie-numerique-le-cameroun-tient-sa-maison-du-digital. Consulté le 15 avril 2022.

[56] Activités Génératrices de Revenus.

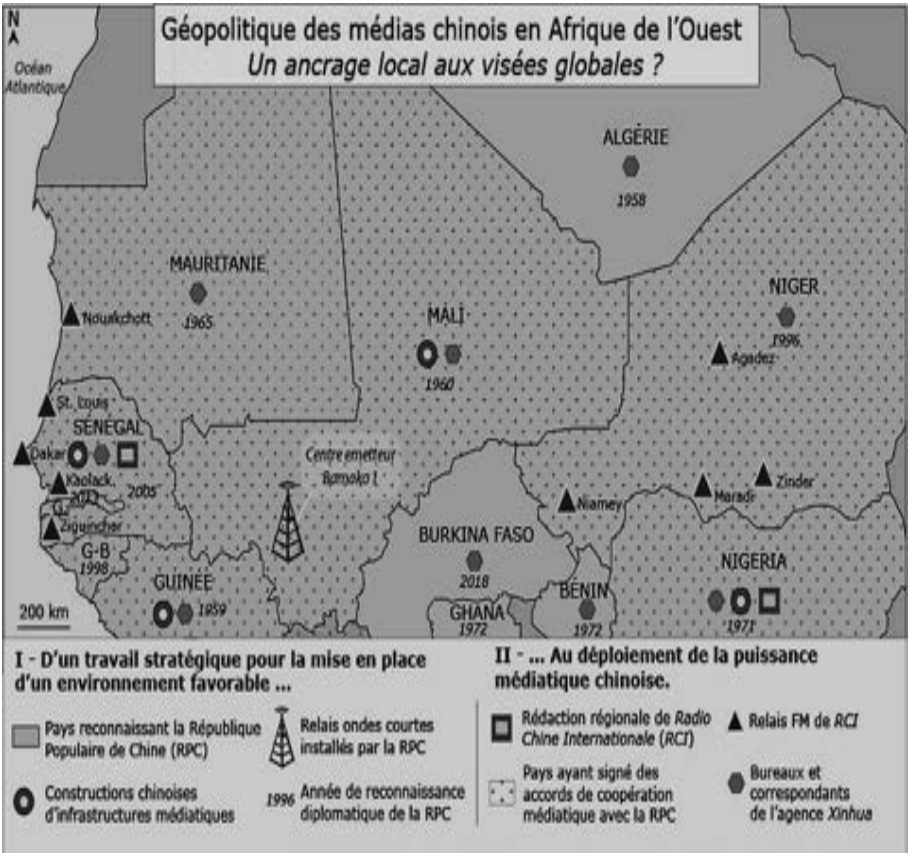
cyberespace constituent des biotopes intéressants pour l'implémentation d'une telle stratégie, qui jouit aussi des avantages sur le plan extérieur.

2 - LES AVANTAGES GÉOPOLITIQUES ET GÉOÉCONOMIQUES D'UNE ÉCONOMIE NATIONALE DES MÉDIAS VIGOUREUSE SUR LE PLAN EXTÉRIEUR

De prime abord, il importe de préciser que la compétitivité économique des Etats africains jouit non seulement d'une dimension interne, c'est à dire la capacité pour les entreprises nationales à satisfaire la demande nationale, mais aussi d'une dimension extérieure en ce sens qu'elle interroge la capacité des Etats africains à faire face aux stratégies économiques développées par les acteurs extérieurs dans l'optique de la maitrise de ce qu'il convient d'appeler «compétition économique mondiale»[57]. Dans ce théâtre compétitif, le secteur des médias et de la communication, spécialisés ou non apparait comme un outil déterminant que mobilisent les acteurs stratégiques dans la perspective d'assurer la réussite de leurs stratégies dans des marchés précis. Dans ce contexte, la mobilisation de l'intelligence économique comme instrument cognitif, et réflexif se pose comme une nécessité et un lieu d'intermédiation servant à «l'élaboration de stratégies collectives – notamment la coopération entre gouvernements et entreprises dans la production de l'avantage concurrentiel – et celle de l'importance de la connaissance dans l'économie et l'industrie comme moteur stratégique du développement et du changement »[58]. Si les plus grandes puissances économiques développent des stratégies d'implantation et de pénétration de leurs industries médiatiques sur le Continent (figures), les stratégies d'internationalisation des média africains restent encore timides.

[57] Lire B. Esambert, La Guerre économique mondiale, Paris, Oliver Orban, 1991.

[58] G. Colletis, «Intelligence économique: vers un nouveau concept en analyse économique ?», Revue d'Intelligence Économique, n° 1, AFDIE, mars 1997, pp. 26-27.


Géopolitique des médias chinois en Afrique de l'Ouest
Un ancrage local aux visées globales ?
N
Océan Atlantique
ALGÉRIE
1958
MAURITANIE
1965
Nouakchott
MALI
1960
NIGER
1996
Agadez
St. Louis
SÉNÉGAL
Dakar
Kaolack
2005
Ziguinchor
G-B
1998
Centre emetteur Bamako I
Niamey
Maradi
Zinder
BURKINA FASO
2018
GUINÉE
1959
GHANA
1972
BÉNIN
1972
NIGERIA
1971
200 km
I - D'un travail stratégique pour la mise en place d'un environnement favorable ...
Pays reconnaissant la République Populaire de Chine (RPC)
Relais ondes courtes installés par la RPC
Constructions chinoises d'infrastructures médiatiques
1996 Année de reconnaissance diplomatique de la RPC
II - ... Au déploiement de la puissance médiatique chinoise.
Rédaction régionale de Radio Chine Internationale (RCI)
Relais FM de RCI
Pays ayant signé des accords de coopération médiatique avec la RPC
Bureaux et correspondants de l'agence Xinhua

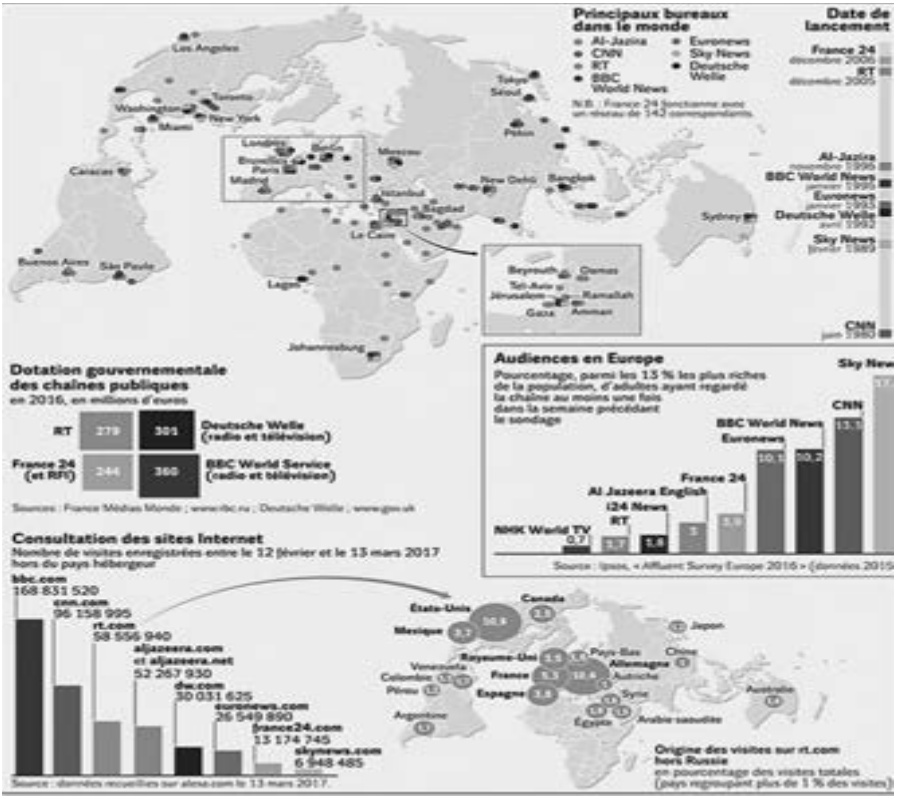


Figure 6 et 7: Géopolitique des médias chinois en Afrique de l'Ouest[59]Les principales chaînes mondiales d'information en continu[60]

Dans ce théâtre, une orientation stratégique des médias sur le plan extérieur permettrait d'avoir deux avantages, à savoir la constitution des niches extérieures de marketing-pays auprès des pays regorgeant de potentiels investisseurs d'une part, et aussi la captation des catégories diasporiques de leurs pays en vue d'offrir à ces dernières des contenus spécifiques à leurs attentes diverses. Pour le premier enjeu, il est principalement question pour les gouvernements africains de se positionner comme des acteurs crédibles dans la fourniture de l'information à caractère économique pour leur pays au sein des plateformes de distribution et de

[59] https://www.diploweb.com/Carte-Geopolitique-des-medias-chinois-en-Afrique-de-l-Ouest-Un-ancrage-local-aux-visees-globales.html. Consulté le 12 avril 2022.

[60] Le Monde diplomatique, Les principales chaînes mondiales d'information en continu,

vulgarisation de l'information économique et financière. En effet, en réussissant ce pari, cela permettrait aux Etats africains de se positionner comme sources d'information susceptibles de fournir une représentation propre des contextes et potentialités économiques de leurs pays respectifs. Nonobstant les économies réalisées pour les campagnes markéting et de renforcement de l'attractivité, la maitrise du message à faire passer constitue un atout stratégique important. Un avantage qui se situe dans une posture synoptique à celui de l'attraction des diasporas.

La diaspora a toujours représenté une forte ressource mobilisable au service du développement socioéconomique et même de la puissance des Etats de manière générale. Si historiquement les diasporas ont toujours constitué à l'extérieure une «monde propre»[61] susceptible de constituer une niche de projection d'influence des Etats, du fait de la proximité linguistique et culturelle[62], elles se posent en véritables instruments du *soft power* mobilisées par plusieurs Etats du monde. Cette option peut aussi être empruntée par les Etats subsahariens dans l'optique d'attirer les composantes diasporiques négro-africaines dans le but de renforcer son économie en développement des stratégies et programmes d'attractivité généraux ou spécifiques. Une mobilisation stratégique du nexus «diasporas, développements et mondialisations»[63] apparait comme la principale difficulté que doit gérer les Etats africains dans l'objectif de mobiliser ces catégories et extensions de la population de l'Etat aux efforts de promotion du développement socioéconomique, puisque celui-ci constitue un des enjeux contemporains les plus déterminants pour les Etats d'Afrique, notamment ceux d'Afrique Noire. Si plusieurs initiatives ont souvent été prises au niveau régional et nationaux, force est de constater que leur impact sur le développement en Afrique est insuffisant et peut être amélioré qualitativement. Voila pourquoi en 2008, «l'Union africaine organisait à Paris une conférence destinée aux diasporas africaines en Europe. Objectif? Trouver de nouvelles voies pour les impliquer davantage dans les politiques de développement des pays et du continent africains»[64]. Ce point de départ

[61] E. Ma Mung, «Continuité temporelle, contiguïté spatiale et création d'un monde-propre. Le cas de la diaspora chinoise»: L'Espace géographique Vol. 41, No. 4 (octobre-novembre-décembre 2012), pp. 352-368 (17 pages)

[62] L'actualité du Conflit russo-ukrainien de 2022 démontre la proximité entre les populations russophones de l'Est de l'Ukraine pro-russes face au gouvernement de Kiev, et la facilité d'acceptation et de mobilisation face aux réfugiés ukrainiens de type caucasien en Europe occidentale, contrairement au rejet des réfugiés d'origines arabo-musulmanes et negro-africaine.

[63] Fibbi, Rosita, et J.-B. Meyer, «Introduction. Le lien plus que l'essence», Autrepart, vol. 22, no. 2, 2002, pp. 5-21.

d'une mobilisation institutionnelle, faite par l'institution faitière de l'Intégration africaine apparait comme un appel en direction des diasporas en vue de se pencher sur les questions développementales en y apportant leur contribution, mais aussi comme un signal pour ces Etats d'investir ce théâtre par le développement des médias ciblant ces catégories précieuses dont le poids économique n'est plus à démontrer. En développant des plateformes médiatiques et communicationnelles orientées vers la vulgarisation des mesures incitatives à l'investissement pour cette catégorie, les Etats africains tireraient à coup sûr des avantages, au-delà de doper la compétitivité économique de leurs Etats.

Au demeurant, on peut dire que face au constat de l'absence des stratégies médias et de communication, dans un contexte global fortement digitalisé[65] caractérisé par la contraction de l'espace-temps[66] et de niches de potentialités variables pour les Etats, les Etats du continent gagneraient dans une option comportementale stratégique, à construire et à élaborer des stratégies susceptibles de renforcer leur attractivité économique. Ces stratégies, dont l'élaboration se doit d'être guidées par les principes de *local contain*[67]*,* et d'ouverture devraient d'abord mettre en avant les mécanismes susceptibles d'influencer de manière significative leurs marchés et leurs opinions nationales sur le plan interne, ensuite leurs permettre de se positionner en sources d'information crédibles pour les potentiels investisseurs extérieurs au niveau régional et global, et enfin capter les diasporas pour attirer ces dernières à investir en Afrique dans plusieurs secteurs économiques. En fin de compte, i contrôler ce que les gens pensent, revient à contrôler les gouts et les options de consommation, il est temps pour les Etats africains d'orienter leur *soft power* vers des stratégies médias et communicationnelles pertinentes pour générer des effets de croissance et de développement socioéconomique. /-

---

[64] Nkrumah Samia, et Habibou Bangré. ««Le bien-être de la diaspora et celui de l'Afrique sont fortement interconnectés»«, Africultures, vol. 72, no. 1, 2008, pp. 130-133.

[65] Lire Obadia L., «Technologies mondialisées, mondialisation technologique, Digital Globalization: quels liens entre les NTIC et la mondialisation ?», Diogène, vol. 271-272, no. 3-4, 2020, pp. 110-132.

[66] Moreau- Desfarges P., *La Mondialisation (Globalisation)*, PUF, coll. «Que sais-je ?», n° 1687, 8e édition, 2010.

[67] Lire à propos Anita Marangoly George's, in *Le contenu local dans les industries extractives, un outil de diversification économique et de développement durable,* https://blogs.worldbank.org/fr/voices/industries-extractives-diversification-economique-et-developpement-durable du 30 janvier 2016. Consulté le 12 Avril 2022.

BIBLIOGRAPHIE

1 **Perez, Stanis**. «9 - Le règne de l'image», Le Corps du roi. Incarner l'État de Philippe Auguste à Louis-Philippe, sous la direction de Perez Stanis. Perrin, 2018, pp. 213-232.

2 **Bernard Eric.** La transmission internet par satellite et l'Afrique: matérialité du système (Internet transmission by satellite and Africa: reality of the system). In: Bulletin de l'Association de géographes français, 78e année, 2001-1 (mars). Réseaux de télécommunications. Périurbanisation en Europe. pp. 17-25

3 **Beckouche, Pierre**. «Chapitre 2. … une révolution économique ?», Les Nouveaux territoires du numérique. L'univers digital du sur-mesure de masse, sous la direction de Beckouche Pierre. Éditions Sciences Humaines, 2019, pp. 33-66

4 **Henri Desbois,** «Le cyberespace», Carnets de géographes [En ligne], 2 | 2011, mis en ligne le 02 mars 2011, consulté le 13 avril 2022.

5 **Margot Beauchamps et Henri Desbois**, «Espaces virtuels», Carnets de géographes [En ligne], 2 | 2011, mis en ligne le 02 mars 2011, consulté le 13 avril 2022

6 **Desforges, Alix**. «Les représentations du cyberespace: un outil géopolitique», Hérodote, vol. 152-153, no. 1-2, 2014, pp. 67-81.

7 **Douzet, Frédérick, et Aude Géry**. «Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace», Hérodote, vol. 177-178, no. 2-3, 2020, pp. 329-350.

8 **Lire Sagna, Olivier**. «La lutte contre la fracture numérique en Afrique: aller au-delà de l'accès aux infrastructures», Hermès, La Revue, vol. 45, no. 2, 2006, pp. 15-24.

9 https://www.agenceecofin.com/industrie/2907-78980-grace-au-numerique-le-continent-africain-est-en-train-de-reduire-son-retard-par-rapport-aux-pays-developpes-huawei. Consulté le 15 avril 2022.

10 **Boulanger, Philippe**. «Bibliographie» , Géopolitique des médias. Acteurs, rivalités et conflits, sous la direction de Boulanger

11 https://www.agenceecofin.com/industrie/2907-78980-grace-au-numerique-le-continent-africain-est-en-train-de-reduire-son-retard-par-rapport-aux-pays-developpes-huawei. Consulté le 15 avril 2022.

12 **Boulanger, Philippe**. «Bibliographie» , Géopolitique des médias. Acteurs, rivalités et conflits, sous la direction de Boulanger Philippe. Armand Colin, 2014, pp. 295-300.

13 **Barrat Jacques**, 1992, Géographie économique des médias, t. 1: «Médias et développement», t. 2: «Diversité des Tiers-Monde», Paris, Litec.

14 **Gaillard, Norbert**. «II. Définition, interprétation, typologie et modalités d'attribution des notations», Norbert Gaillard éd., Les agences de notation. La Découverte, 2010, pp. 16-42.

15 https://www.rfi.fr/fr/podcasts/afrique-%C3%A9conomie/20210906-les-agences-africaines-de-notation-financi%C3%A8re-commencent-%C3%A0-%C3%AAtre-prises-au-s%C3%A9rieux. Consulté le 13 avril 2022.

16 **Bourgain, Arnaud, Jean Brot, et Hubert Gérardin**. «L'attractivité: quel levier pour le développement ?», Mondes en développement, vol. 149, no. 1, 2010, pp. 7-10.

17 Africa24, Etudes: Audiences et donnes: 2020.

18 Idem.

19 https://www.telesatellite.com/actu/50279-le-top-10-des-chaines-les-plus-regardees-en-afrique-francophone.html

20 MÉCHINAUD Coline, L'Afrique de l'Ouest dans le cyberespace: enjeux de sécurité et de souveraineté, Note d'Analyse du GRIP,19 novembre 2019, Bruxelles.

21 **Muet, Pierre-Alain.** «Impacts économiques de la révolution numérique», Revue économique, vol. 57, no. 3, 2006, pp. 347-375.

22 **Éric Chaplet**, «La souveraineté économique au service de la souveraineté nationale:», Revue Dé-

fense Nationale, vol. N° 801, no 6

23 **Martel, Frédéric. Mainstream**. Enquête sur la guerre globale de la culture et des médias. Flammarion, 2020

24 **Devin, Guillaume**. «II. La définition de la puissance», Guillaume Devin éd., *Sociologie des relations internationales*. La Découverte, 2013, pp. 29-36.

25 **Hoffmann, Stanley**. «Raymond Aron et la théorie des relations internationales», Politique étrangère, vol. , no. 4, 2006, pp. 723-734.

26 **Champagne (Patrick)**, Faire l'opinion. Le nouveau jeu politique, Paris, Minuit, coll. «Le sens commun», 1990;

27 **Belaid, Samy**. «L'image du Pays. Proposition d'une échelle de mesure», La Revue des Sciences de Gestion, vol. 222, no. 6, 2006, pp. 141-147.

28 **Bomsel, Olivier**. «Qu'est-ce que le numérique ?», Entreprises et histoire, vol. 43, no. 2, 2006, pp. 5-14.

29 **Rochette, Corinne**. «Le marketing territorial: comment développer l'attractivité et l'hospitalité des territoires ? **Chamard C.** (sous la direction), Préface de Rousset A., avec la collaboration de Gayet J. et Alaux C., et la participation de Gollain V. et Boisvert Y. (2014), 203 pages, ISBN 978-2-8041-8472-8», Gestion et management public, vol. 6/1, no. 3, 2017, pp. 77-80.

30 **Descartes**, Œuvres, éd. Adam/Tannery, t. vi, p. 62.

31 Office de radiotélévision à capitaux publics du Cameroun.

32 La Société de Presse et d'Éditions du Cameroun édite plusieurs titres de journaux à capitaux publics proches du gouvernement camerounais parmi lesquels on peut citer: *Cameroon Tribune*, Weekend *Sports* et Loisirs, *Nyanga,* et *Cameroon Business Today*.

33 Le *Nigerian Television Authority* est le groupe audiovisuel public de la République Fédérale du Nigeria.

34 Il s'agit principalement des Etats de la *zone franc* d'Afrique de l'Ouest et du Centre.

35 Roux, Dominique. «La création des entreprises», Dominique Roux éd., Les 100 mots de la gestion. Presses Universitaires de France, 2011, pp. 7-15.

36 **Ben Hamadi, Zouhour, Philippe Chapellier, et Fabienne Villesèque-Dubus**. «Innovations budgétaires en PME: l'influence du secteur d'activité et du profil du dirigeant», Innovations, vol. 43, no. 1, 2014, pp. 223-252.

37 Attitude des pouvoirs publics camerounais qui restent peu regardantes sur les exigences administratives requises pour certains usages socioéconomiques régies par la loi et la règlementation.

38 **Gallic, Claire, et Rémy Marrone**. «Chapitre 2. Les modèles économiques», Le grand livre du marketing digital. Sous la direction de Gallic Claire, Marrone Rémy. Dunod, 2020, pp. 27-43.

39 **Belaid, Samy**. «L'image du Pays. Proposition d'une échelle de mesure», La Revue des Sciences de Gestion, vol. 222, no. 6, 2006, pp. 141-147.

40 **Lecat, Benoît**. «Comment promouvoir son pays, sa région ou sa ville auprès des investisseurs étrangers ? Identification des critères d'implantation et de leur importance par l'entremise du marketing public», Reflets et perspectives.

41 **Chartoire, Renaud**. «Analyser les niches fiscales», Idées économiques et sociales, vol. 166, no. 4, 2011, pp. 39-47.

42 **Bourgain, Arnaud, Jean Brot, et Hubert Gérardin**. «L'attractivité: quel levier pour le développement ?», Mondes en développement, vol. 149, no. 1, 2010, pp. 7-10.

43 Lire **Sourbès-Verger, Isabelle**. «Espace et géopolitique», L'Information géographique, vol. 74, no. 2, 2010, pp. 10-35.

44 **Sonnac, Nathalie**. «Les médias: une industrie à part entière et entièrement à part», Questions de communication, vol. 9, no. 1, 2006, pp. 455-473.

45 EL QOUR, T., BELFAHMI, B., «L'internationalisation des entreprises publiques comme outil d'intégration africaine: le biais de la diplomatie économique. Analyse de cas marocains», Revue «Repères et Perspectives Economiques» [En ligne], Vol. 4, Numéro spécial / novembre 2020, mis

en ligne le 26 novembre 2020.

46 **Dosquet, Frédéric**. «Chapitre 1. Les missions des études de marché», Frédéric Dosquet éd., Études de marché. Dunod, 2018, pp. 1-35.

47 *Bloomfield Investment* est la toute 1ère Agence de Notation Financière d'Afrique Francophone situé en Cote d'Ivoir. Elle fut créée en 2007.

48 https://www.sikafinance.com/marches/l-ua-va-creer-sa-propre-agence-de-notation-financiere_33700. Consulté le 12 avril 2022.

49 **Giry, Julien**. Les fakes news comme concept de sciences sociales. Essai de cadrage à partir de notions connexes: rumeurs, théories du complot, propagande et désinformation», Questions de communication, vol. 38, no. 2, 2020, pp. 371-394.

50 **Mathieu-Castellani, Gisèle**. «Devis/récits: le cadre et le contrat narratif», , La conversation conteuse. Les nouvelles de Marguerite de Navarre, sous la direction de Mathieu-Castellani Gisèle. Presses Universitaires de France.

51 **Rossignol, Jean-Luc**. «Fiscalité et responsabilité globale de l'entreprise», Management & Avenir, vol. 33, no. 3, 2010, pp. 175-186.

52 **Frère, Marie-Soleil**. «Chapitre 6. L'économie des médias en Afrique francophone», , Journalismes d'Afrique. Sous la direction de Frère Marie-Soleil. De Boeck Supérieur, 2020, pp. 259-300.

53 Lire **ATENGA Thomas, MADIBA Georges** (2012), La communication au Cameroun: les objets, les pratiques, Paris, Archives Contemporaines Editions, 180 p.

54 **Sonnac, Nathalie, et Jean Gabszewicz.** «IV. Marchés et stratégies des médias à l'ère numérique», Nathalie 53 Sonnac éd., L'industrie des médias à l'ère numérique. La Découverte, 2013, pp. 57-84.

55 **Alain François LOUKOU**, «Les TIC au service du développement en Afrique», tic&société Vol. 5, n°2-3 | 2e sem. 2011 / 1er sem. 2012, avril 2019.

56 https://www.minpostel.gov.cm/index.php/fr/actualites/407-economie-numerique-le-cameroun-tient-sa-maison-du-digital. Consulté le 15 avril 2022.

57 Activités Génératrice de Revenus.

58 Lire **B. Esambert**, La Guerre économique mondiale, Paris, Oliver Orban, 1991.

59 **G. Colletis**, «Intelligence économique: vers un nouveau concept en analyse économique ?», Revue d'Intelligence Économique, n° 1, AFDIE, mars 1997, pp. 26-27.

60 https://www.diploweb.com/Carte-Geopolitique-des-medias-chinois-en-Afrique-de-l-Ouest-Un-ancrage-local-aux-visees-globales.html. Consulté le 12 avril 2022.

61 Le Monde diplomatique, Les principales chaînes mondiales d'information en continu,

62 **Emmanuel Ma Mung,** «Continuité temporelle, contiguïté spatiale et création d'un monde-propre. Le cas de la diaspora chinoise»: L'Espace géographique Vol. 41, No. 4 (octobre-novembre-décembre 2012), pp. 352-368 (17 pages)

63 L'actualité du Conflit russo-ukrainien de 2022 démontre la proximité entre les populations russophones de l'Est de l'Ukraine pro-russes face au gouvernement de Kiev, et la facilité d'acceptation et de mobilisation face au réfugiés ukrainiens de type caucasien en Europe occidentale, contrairement au rejet des réfugiés d'origines arabo-musulmanes s et negro-africaine.

64 **Fibbi, Rosita, et Jean-Baptiste Meyer**. «Introduction. Le lien plus que l'essence», Autrepart, vol. 22, no. 2, 2002, pp. 5-21.

65 **Nkrumah, Samia, et Habibou Bangré.** ««Le bien-être de la diaspora et celui de l'Afrique sont fortement interconnectés»«, Africultures, vol. 72, no. 1, 2008, pp. 130-133.

66 Lire **Obadia, Lionel**. «Technologies mondialisées, mondialisation technologique, Digital Globalization: quels liens entre les NTIC et la mondialisation ?», Diogène, vol. 271-272, no. 3-4, 2020, pp. 110-132.

67 **Moreau- Desfarges, Philippe**, *La Mondialisation (Globalisation)*, PUF, coll. «Que sais-je ?», n°

1687, 8e édition, 2010.

68 Lire à propos **Anita Marangoly George's**, in *Le contenu local dans les industries extractives, un outil de diversification économique et de développement durable,* https://blogs.worldbank.org/fr/voices/industries-extractives-diversification-economique-et-developpement-durable du 30 janvier 2016. Consulté le 12 Avril 2022.

69 G. Colletis, «Intelligence économique: vers un nouveau concept en analyse économique ?», Revue d'Intelligence Économique, n° 1, AFDIE, mars 1997, pp. 26-27.

70 https://www.diploweb.com/Carte-Geopolitique-des-medias-chinois-en-Afrique-de-l-Ouest-Un-ancrage-local-aux-visees-globales.html. Consulté le 12 avril 2022.

71 Le Monde diplomatique, Les principales chaînes mondiales d'information en continu,

72 Emmanuel Ma Mung, «Continuité temporelle, contiguïté spatiale et création d'un monde-propre. Le cas de la diaspora chinoise»: L'Espace géographique Vol. 41, No. 4 (octobre-novembre-décembre 2012), pp. 352-368 (17 pages)

73 L'actualité du Conflit russo-ukrainien de 2022 démontre la proximité entre les populations russophones de l'Est de l'Ukraine pro-russes face au gouvernement de Kiev, et la facilité d'acceptation et de mobilisation face aux réfugiés ukrainiens de type caucasien en Europe occidentale, contrairement au rejet des réfugiés d'origines arabo-musulmanes s et negro-africaine.

74 Fibbi, Rosita, et Jean-Baptiste Meyer, «Introduction. Le lien plus que l'essence», Autrepart, vol. 22, no. 2, 2002, pp. 5-21.

75 Nkrumah Samia et Habibou Bangré, «Le bien-être de la diaspora et celui de l'Afrique sont fortement interconnectés»«, Africultures, vol. 72, no. 1, 2008, pp. 130-133.

76 Lire Obadia Lionel, «Technologies mondialisées, mondialisation technologique, Digital Globalization: quels liens entre les NTIC et la mondialisation ?», Diogène, vol. 271-272, no. 3-4, 2020, pp. 110-132.

77 Moreau- Desfarges Philippe, *La Mondialisation (Globalisation)*, PUF, coll. «Que sais-je ?», n° 1687, 8e édition, 2010.

78 Lire à propos Anita Marangoly George's, in *Le contenu local dans les industries extractives, un outil de diversification économique et de développement durable,* https://blogs.worldbank.org/fr/voices/industries-extractives-diversification-economique-et-developpement-durable du 30 janvier 2016. Consulté le 12 Avril 2022.

PANEL 3: INTERNET ET MÉDIAS SOCIAUX: DE L'ÉTAT DE NATURE AU RETOUR À L'ORDRE

LA REPRESSION DES ACTEURS CYBER-ACTIFS POTENTIELLEMENT DANGEREUX: FORCES ET FAIBLESSES DES MECANISMES EXISTANTS

Thierry MEDOU
Commissaire Divisionnaire, Ph.D en droit public,
Commissaire Central n°1 de la ville de Yaoundé

RESUME

La généralisation, voire la démocratisation des nouvelles technologies de l'information et de la communication est une formidable opportunité non seulement pour les institutions publiques ou privées, mais aussi pour les individus des pays en développement comme le Cameroun. En même temps, elle constitue l'une des plus grosses menaces qui pèsent sur ces entités au regard de l'usage qu'en font certains individus malveillants, lesquels ont, par ce canal, plus de facilités pour leur faire du tort. Le Cameroun a fini par prendre conscience du danger que représente cet usage malveillant de la cybercriminalité et a mis en œuvre des mécanismes textuels, institutionnels et dans, une moindre mesure, infrastructurels pour y faire face. Toutefois, le dispositif ainsi mis en place a besoin de la coopération extérieure, au-delà du fait qu'il doit sans cesse s'ajuster et se réinventer.

INTRODUCTION

Les Technologies de l'Information et de la Communication (TIC) s'appréhendent comme étant «l'ensemble des technologies permettant de traiter des informations numériques et de les transmettre. L'expression «nouvelles technologies de l'information et de la communication» désigne donc une combinaison d'informatique et de télécommunications, mais elle s'est spécialement répandue dans le contexte du réseau internet et du multimédia, c'est-à-dire de l'information audiovisuelle numérisée (images et sons, par opposition aux données de type texte et chiffres, moins volumineuses, qui constituaient l'essentiel des données transitant par les réseaux jusqu'au développement du web et du protocole http)»[1].Ainsi présentées, les TIC s'agrègent autour de l'Internet qui met en relation une communauté virtuelle d'utilisateurs.

On le voit donc et pour le dire en des mots simples, les TIC et le moteur qui les porte, à savoir l'internet, ont été créés pour faciliter la vie aux utilisateurs. Malheureusement pour la société s'ils sont dans leur très grande majorité bienveillants, une frange des utilisateurs de ces outils sont malveillants et même potentiellement dangereux. En effet, l'évolution fulgurante de l'internet a crée de nouvelles opportunités pouvant permettre à cette dernière catégorie de se livrer à des activités de cybercriminalité à grande échelle. La conséquence en est qu'aujourd'hui, tout le monde est exposé aux cyberattaques: les Etats, les institutions nationales publiques et privées, les entreprises, les institutions internationales publiques et privées, les ONG[2] et toutes les catégories des populations. Celles-ci sont perpétrées dans tous les types de plateformes et équipements numériques.

La thématique examinée ici semble, de prime abord, laisser planer certaines ambiguïtés qu'il importe de balayer au plus vite. La première ambiguïté porte sur l'expression «acteurs cyberactifs potentiellement dangereux». En effet, cette expression pourrait s'appliquer au final à tous les utilisateurs réguliers d'internet qui sont tous potentiellement dangereux, car même s'ils ne le font pas, ils ont, de par leur savoir faire, la capacité d'en

[1] https://www.dictionnaire-juridique.com/definition/ntic-nouvelles-technologies-de-l-inf... Consulté le 21 avril 2022 à 22H22'.

[2] Organismes non gouvernementaux

faire un usage malveillant ou criminel. Aussi, pour ne pas nous attarder sur des questions de sémantique non intéressantes, qu'il soit clairement entendu ici que cette expression renvoie tout simplement aux utilisateurs «malveillants» de l'outil internet.

La seconde ambiguïté porte sur l'espace auquel renvoi cette thématique, lequel, en l'état, semble extrêmement vaste puisqu'il commande d'examiner «tous» les mécanismes existants pour réprimer les utilisateurs malveillants des TIC à travers le monde. Aussi, nous contenterons nous ici de n'analyser que les mécanismes existants au Cameroun, le recours ou la référence à un mécanisme existant ailleurs n'étant faite que pour mieux mettre en lumière la situation propre à ce pays.

Dans une démarche définitionnelle, nous retenons dans la présente étude que l'expression «Répression» qui rend fondamentalement compte d'une action exercée sur autrui peut être présentée comme étant «l'action de réprimer, de prendre des mesures punitives contre ceux qui sont jugés contrevenir aux règles, aux lois ou aux options d'un gouvernement, d'une société ou à la morale»[3].

Les «acteurs cyberactifs», quant à eux, sont des utilisateurs non pas occasionnels, mais réguliers du cyberespace, lequel est «un domaine global constitué du réseau maillé des infrastructures, des technologies de l'information (dont internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne»[4]. Cette définition retenue par la doctrine de défense française nous semble plus globale, puisqu'elle prend en compte le cyberespace dans toutes ses dimensions à savoir virtuelle, réelle, physique (infrastructures d'internet à savoir entre autres serveurs racines, bases des données, satellites, câbles sous-marins, fibres optiques), logique (logiciel et protocoles du réseau), cognitive (ensemble des données, des informations, du contenu circulant au sein du réseau)[5].

Dans ce cyberespace, des utilisateurs réguliers posent au quotidien des actes malveillants que l'on regroupe sous le vocable «cybercrimes». Comme

[3] https://www.cnrtl.fr/definition/repression consulté le 23 avril 2022 à 20h33'.
[4] B. Louis-Sidney, «La dimension juridique du cyberespace», Revue internationale et stratégique 2012/3 (No87), pp73-81.
[5] Ibid.

tous les autres Etats, le Cameroun enregistre de nombreux actes de cybercriminalité, laquelle se définit comme étant l'«ensemble des infractions s'effectuant à travers le cyberespace par d'autres moyens que ceux habituellement mis en œuvre, et, de manière complémentaire à la criminalité classique»[6].

Pour sa part, le mot «mécanisme» est présenté comme étant une «combinaison, un agencement de pièces, d'organes, montés en vue d'un fonctionnement, ou encore comme un dispositif constitué par des pièces assemblées ou reliées les unes aux autres ou remplissant une fonction déterminée»[7]. C'est donc dire que le mot mécanisme dans ce cadre renvoie simplement à tout ce qui est conçu et mis ensemble pour lutter contre la cybercriminalité au Cameroun, le point d'emphase étant que les dispositifs ainsi créés aient un lien entre eux. En effet, l'idée ici est qu'aucun des dispositifs de lutte contre la cybercriminalité au Cameroun ne suffit à lui seul pour faire le tour de la question, puisqu'ils sont tous complémentaires, de sorte que soit en amont, soit concomitamment, soit en aval, chacun de ceux-ci exploite, car en ayant besoin, le travail des autres.

En effet, pour les autorités camerounaises, la cybercriminalité dans ce pays est une réalité qu'on ne saurait plus ni occulter, ni négliger au regard de ses conséquences pour l'image de celui-ci[8], d'une part, mais aussi des enjeux de la lutte contre la cybercriminalité[9], d'autre part. Elles ont donc pris

---

[6] Loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, article 4, point 32.

[7] https://www.larousse.fr»français, consulté le 19 avril 2022 à 22h40'.

[8] Dans ce sens, le rapport de la société de sécurité informatique MCAfee publié en 2011 indiquait déjà que le «.cm» du Cameroun fait partie des cinq noms de domaine les plus risqués à côté des «.com», «.cn», «.ws», «.info», avec un taux de risque de 36,7 %, sur environ 27 millions de noms de domaines analysés tel qu'indiqué dans un article du site agenceecofin.com, https://www.agenceecofin.com/?option=com_k&2id=3266&view=item&itemid=181&tmpl=c... Consulté le 21 avril 2022 à 1h 20'.

[9] En effet, les enjeux de la lutte contre la cybercriminalité sont d'une très grande importance. Bien que très nombreux, nous n'en développons ici que trois des principaux à savoir;

-son coût, car les victimes perdent énormément d'argent. Selon l'ANTIC, la cybercriminalité a coûté 3 milliards aux banques en 2015, et depuis 2010, les victimes du Scaming au Cameroun ont perdu 7 milliards, celles du phising 4 milliards et celles du skimming 3 milliards.

-La sécurité de l'Etat et des systèmes d'information qui sont menacés. Un rapport du ministère des postes et des télécommunications révèle qu'en 2010 par exemple, le site officiel du premier ministre a été piraté, puis plus tard, le ministère du domaine, du cadastre et des affaires foncières. Des journaux importants comme Cameroun tribune ou mutations aussi.

-Les droits des personnes qui sont facilement violés à travers des intrusions cybercriminelles dans leur vie privée.

conscience de la nécessité d'élaborer des mécanismes efficaces de lutte contre celle-ci, laquelle se traduit effectivement par la mise en place de nombreux mécanismes dédiés à cette lutte, dont il importe d'évaluer l'efficacité. La question devient donc: **Quelle évaluation peut-on faire des dispositifs de lutte contre la cybercriminalité au Cameroun en termes d'efficacité ?**

La recherche des réponses à cette question impose de mettre en lumière les forces et les faiblesses des mécanismes ou dispositifs existants au Cameroun pour lutter contre la cybercriminalité, lesquels sont normatifs, institutionnels et infrastructurels. Bien qu'importantes, les questions infrastructurelles seront abordées dans le volet des recommandations qui constituent l'essentiel de notre propos conclusif. La priorité est donc donnée aux mécanismes normatifs, d'une part (I), et aux mécanismes institutionnels, d'autre part (II), deux volets qui nous semblent davantage plus complexes et dont l'appréhension est fondamentale dans une perspective évaluative de la lutte contre la cybercriminalité au Cameroun.

I - DES MECANISMES NORMATIFS A PARFAIRE

La lutte contre la cybercriminalité au Cameroun est organisée par un ensemble de textes qui se caractérisent par une volonté affichée de ratisser large et de prendre en compte le plus grand nombre possible d'actes cybercriminels (A), ce qui transparaît clairement des incriminations retenues, lesquelles se veulent particulièrement dissuasives (B).

A - DES TEXTES DIVERS AMBITIONNANTS UNE LARGE APPREHENSION DE LA LUTTE CONTRE LA CYBERCRIMINALITE

Ils sont internationaux et communautaires, d'une part (1), et nationaux, d'autre part (2). En effet, comme rappelé dans l'article 2(1) du code pénal camerounais[10], tout comme les textes nationaux, «les règles de droit international, ainsi que les traités dûment promulgués et publiés, s'imposent au présent code, ainsi qu'à toute disposition pénale».

[10] Loi N°2016/007 du 12 juillet portant code pénal

LES TEXTES INTERNATIONAUX ET COMMUNAUTAIRES ET LEUR INTERNALISATION AU CAMEROUN

Outre l'état des lieux qui donne une indication des textes internationaux et communautaires organisant la lutte contre la cybercriminalité au Cameroun, il s'agit ici d'en dégager les forces et les faiblesses.

A - L'ÉTAT DES LIEUX

Les fondements juridiques internationaux de la lutte contre la cybercriminalité au Cameroun sont soit directs[11] soit indirects[12].

Du point de vue communautaire, il n'existe pratiquement pas de texte qui mette en place une organisation communautaire de la lutte contre la cybercriminalité, excepté peut-être le texte qui organise la coopération judiciaire dans la zone de la Communauté Monétaire et Economique de l'Afrique Centrale (CEMAC)[13], ainsi que celui qui organise la coopération policière dans le même espace[14], avec la remise des criminels de police à police qui en est une mesure phare[15]. Ces textes favorisent la coopération, car omme on le verra, du fait de la nature souvent internationale des infractions commises, la lutte contre la cybercriminalité doit reposer sur la coopération des acteurs de cette lutte.

---

[11] Ce sont des conventions adoptées uniquement et spécifiquement pour lutter contre la cybercriminalité comme la Convention de Budapest sur la cybercriminalité, adoptée en Hongrie le 23 Novembre 2001 et la Convention de l'Union Africaine sur la Cyber sécurité et la protection des données, adoptée à Malabo le 23 juin 2014.

[12] Il s'agit de conventions adoptées avec d'autres objectifs que celui de traiter du cyberespace et donc de lutter contre la cybercriminalité, certaines datant d'avant l'avènement de la cybercriminalité, mais dont certaines dispositions s'avèrent utiles de nos jours dans le combat contre la ce phénomène. C'est le cas par exemple de la DUDH, du pacte international relatif aux droits civils et politiques, de la convention de l'UIT de 1992, de la constitution de l'UIT de 1992, des règlements des radiocommunications de 2007, de la convention sur l'emploi de la radiodiffusion dans l'intérêt de la paix de 1936, de la convention de Montego Bay de 1982, de la convention internationale relative à la protection des câbles sous-marins de 1884, du traité de l'espace de 1967, de l'accord de Bangui du 2 mars 1977 révisé le 24 février 1999 instituant l'organisation africaine de la propriété intellectuelle qui traite des violations des droits d'auteur, y compris sur internet, etc.

[13] Accord de coopération judiciaire entre les Etats membres de la CEMAC du 28 janvier 2004 à Brazzaville qui pose clairement en son article 2 le principe de l'obligation de l'entraide judiciaire en zone CEMAC.

[14] Accord de coopération en matière de police criminelle entre les Etats de l'Afrique centrale du 18 septembre 2015 à Yaoundé.

[15] En effet, elle permet aux pays de la CEMAC de s'affranchir dans le cadre des enquêtes policières des lourdeurs et contraintes, voire des difficultés de la procédure d'extradition pour remettre à un autre pays membre un malfrat de sa nationalité recherché par celui-ci et qui se serait retrouvé dans le pays remettant.

B - FORCES ET FAIBLESSES

La principale force de ces textes c'est que mis en œuvre, ils donnent aux pays membres les moyens de faire face aux réticences et à la toute puissance des GAFAM[16] qui rechignent parfois à apporter l'aide sollicitée par les Etats, même les plus grands, dans leur lutte contre la cybercriminalité[17]. En effet, des mécanismes y sont prévus pour obliger ces majors du numérique à plier face aux demandes des Etats membres, notamment dans la convention de Budapest.

Pour ce qui est des faiblesses, la plus grande est qu'à date, les textes internationaux fondateurs et majeurs de la lutte contre la cybercriminalité que sont celui de Budapest et sur un plan régional celui de Malabo évoqués plus haut ne sont pas encore intégrés dans notre dispositif normatif, puisque non encore ratifiés au Cameroun. Nous les avons cependant cités ici non seulement parce qu'ils inspirent, malgré tout, les textes nationaux, mais aussi parce qu'ils sont en voie de ratification dans ce pays, puisque la cession de mars 2022 du parlement de ce pays a habilité le Président de la République à ratifier ces deux textes, ce qui ne saurait tarder.

2 - SUR LE PLAN NATIONAL

Ici aussi, il importe, d'une part, d'examiner l'état des lieux de la législation nationale de lutte contre la cybercriminalité (a), et d'autre part, ses forces et ses faiblesses (b).

A - ETAT DES LIEUX

Un effort certain a été fait pour bâtir une armature juridique crédible de lutte contre la cybercriminalité, mais de nombreux aspects de celle-ci n'ont pas été pris en compte par le législateur, à l'exemple de la protection des données personnelles. Néanmoins, sur le plan national, le schéma est le même que sur la scène internationale avec des textes directement dédiés à la lutte contre la

[16] Il s'agit d'un acronyme pour désigner les principales entreprises du monde du numérique à savoir, Google, Apple, Facebook, Amazon et Microsoft.

[17] Le 17 février 2016, la société Apple a publié une lettre de refus d'exécuter une décision d'un juge américain lui ordonnant d'aider le FBI à débloquer un Iphone dans le cadre de l'affaire du tueur de San Bernadino.

cybercriminalité[18] et d'autres qui le sont indirectement[19], mais tout aussi utilement. Bien évidemment, cette armature juridique a des forces et des faiblesses.

B - FAIBLESSES ET FORCES

Pour ce qui est des faiblesses, nous en retenons quelques-unes des plus importantes:

Premièrement, la disparité des législations nationales, ce qui fait qu'un comportement catégorisé comme étant une infraction cybercriminelle au Cameroun peut ne pas être incriminé dans un autre pays, ce qui est source de complications quand une procédure cybercriminelle comporte des éléments d'extranéité.

Deuxièmement les vides juridiques sur de nombreux points. Il existe en effet de nombreux types d'infractions sur internet qui ne sont pas formellement pris en compte par les textes nationaux de lutte contre la cybercriminalité et sanctionnés à ce titre, ceci pour de multiples raisons, comme, par exemple, le taux bas de ce type d'infractions au Cameroun, la lenteur de prise en compte ou une prise de conscience tardive de leur nocivité, ou tout simplement les moyens insuffisants. On note ces vides, par exemple s'agissant de l'usurpation d'identité sur Internet, la vengeance pornographique, l'escroquerie à l'aide des réseaux sociaux, les fake-news, le droit à l'image, la protection des données à

[18] C'est le cas de la Loi N° 2010/012 du 21 décembre 2010 relative à la Cyber sécurité et à la Cybercriminalité, la Loi N° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, modifiée et complétée par la loi N°2015/006 du 20 avril 2015, la Loi N° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun, la Loi N° 2015/006 du 20 avril 2015 régissant l'activité Audiovisuelle au Cameroun.

[19] A titre d'exemple, nous avons la Loi N° 2016-7 du 12 juillet 2016 portant code pénal, qui fixe certaines peines en matière de cybercriminalité; la Loi n° 2005/007 du 27 juillet 2005 portant code de procédure pénale qui organise la poursuite des infractions en matière de cybercriminalité: la loi No 90/052 u 19 décembre 1990 relative à la liberté de communication sociale, modifiée par la loi No 96/04 du 4 janvier 1996:.le décret No 2000/158 du 3 avril 2000 fixant les conditions et les modalités de création et d'exploitation des entreprises privées de communication audiovisuelle, puisque internet est assimilé au Cameroun à un moyen de communication audiovisuelle et soumis de ce fait à ces lois: la loi No 2014/028 du 23 décembre 2014 portant répression des actes de terrorisme qui sanctionne par exemple l'apologie du terrorisme y compris sur internet,: le décret No 2013/0404/PM du premier ministre du 27 février 2013 précisant les modalités de gestion des ressources de nommage et d'adressage (sur internet au Cameroun): la loi No 2006/018 du 29 décembre 2006 régissant la publicité au Cameroun qui détermine les règles relatives au contenu des messages publicitaires 'même sur internet): la loi No 2017/012 du 12 juillet 2017 portant code de justice militaire qui définit entre autres certaines infractions constatées uniquement par les OPJ militaires: la loi No 2000/11 du 19 décembre 2000 relative aux droits d'auteurs et aux droits voisins, laquelle vise à protéger les auteurs, les artistes interprètes, les producteurs de phonogrammes et de vidéogrammes et les entreprises de communication audiovisuelle.

caractère personnel. Il faut cependant se réjouir de ce que le législateur semble avoir résolument pris la mesure de cet impératif, car dans nombre de ces domaines, des textes sont soit en cours d'élaboration, soit déjà élaborés et soumis aux plus hautes instances du pays pour suite de la procédure ou transmission au parlement. Il s'agit par exemple du projet de loi sur la protection des Données à caractère personnel, du projet de loi portant charte de protection des enfants en ligne, de la modification de la loi n°2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité pour corriger certaines de ses insuffisances[20].

Troisièmement, la non précision dans le dispositif juridique de lutte contre la cybercriminalité des process et moyens d'investigations numériques. Il s'agit ici d'une source potentielle de contestation des preuves réunies dans le cadre des investigations numériques. En effet, se pose ici la question de la légalité ou de l'admissibilité des moyens utilisés pour obtenir des preuves numériques. Il n'existe pas de dispositions spécifiques liées aux investigations numériques qui soient clairement précisées dans l'arsenal juridique, à l'instar du code de procédure pénale qui en traite clairement dans le cadre de la criminalité traditionnelle. Dans la pratique, les intervenants de la chaine judiciaire essayent d'étendre aux investigations numériques les dispositions régissant les moyens de preuve dans la criminalité traditionnelle, mais du fait des spécificités du monde numérique, cette extension n'est pas toujours techniquement aisée ou acceptable. Toutefois, pour contourner cette difficulté certains textes internes ont intégré dans leur contenu des dispositions de procédure pénale[21].

La principale force de ces textes est qu'ils sont suffisamment dissuasifs,

[20] En effet, cette mise à jour du texte de 2010 ambitionne de prendre en compte des modes opératoires cybercriminels bien connus sous d'autres cieux mais qui pendant longtemps étaient très peu répandus au Cameroun à l'instar du cyberchantage pornographique, de la cyberpornographie, le phishing, le scamming, le webdefacement dont on veut spécifier et durcir le régime. Elle vise aussi à renforcer les pouvoirs de l'ANTIC, à spécifier le régime des sanctions administratives et pénales, à incriminer les atteintes aux moyens de payement, les atteintes au bien, les atteintes aux données, les atteintes aux systèmes d'information. Il est aussi question d'y encadrer les atteintes liées aux missions d'audit de sécurité, ainsi que les infractions liées aux activités des prestataires techniques des services de communication électronique. Avec la ratification prochaine de la convention de Budapest, il sera nécessaire d'enrichir encore ces propositions de modification qui datent de 2018.

[21] C'est le cas par exemple de la loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun dans ses articles 49, 50, 52(1), 53(1), 55 (2), 56, 58 (1), 88 (1), 88 (2), ou de l'article 6 (3) du décret N° 2012/180 du 10 avril 2012 portant organisation et fonctionnement de l'Antic, ou encore de l'article 11 de la loi N°2017/012 du 12 juillet 2017 portant code de justice militaire.

car très souvent, tant le quantum des peines que le montant des amendes à infliger sont très élevés[22], et cette sévérité transparaît déjà du type d'incriminations retenues.

B - DES INCRIMINATIONS TOURNEES VERS LA DISSUASION

L'utilisation malveillante de l'outil internet peut revêtir plusieurs formes que nous pouvons regrouper en cinq principales catégories.

1 - LA CRIMINALITÉ ÉCONOMIQUE OU FINANCIÈRE OU «CRIMINALITÉ EN COL BLANC»

Les infractions financières se commettent aussi bien sur les particuliers que sur les entreprises, les organisations et les Etats. Les exemples donnés ici pourraient tout aussi bien être insérés dans les atteintes aux personnes, mais par souci d'organisation des idées, nous les étudions ici.

A - LES ESCROQUERIES EN LIGNE

A l'exploitation d'une notice de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) rendant compte de son action pour renforcer la cybersécurité et lutter contre la cybercriminalité au Cameroun, les types d'escroqueries en ligne les plus fréquents au Cameroun sont: le scamming[23], le phishing ou hameçonnage[24], le skimming[25], l'usurpation

[22] A titre d'exemple, dans la loi du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité, l'article 65 punit l'accès et le maintien frauduleux dans un système de traitement automatisé d'un emprisonnement de 5 à 10 ans et d'une amende de 5 à 10 millions, tandis que l'article 68 du même texte sanctionne de 5 à 1à ans de prison et d'une amende de 10 à 50 millions ou de l'une de ces deux peines celui qui pose entrave au fonctionnement d'un système. Dans la même veine, l'article 66 de la même loi sanctionne l'introduction frauduleuse de données et la falsification ou la suppression frauduleuse de données de 2 à 5 ans de prison et de 1 à 2 millions d'amende.

[23] Il s'agit des arnaques perpétrées au moyen des outils TIC qui représentent 80% des cas de cybercriminalité au Cameroun, selon l'ANTIC.

[24] Technique consistant à hameçonner un usager en usurpant l'adresse email ou le site web d'une structure reconnue. Selon l'ANTIC, cette technique représente 15% des cybercrimes au Cameroun.

[25] Technique de fraude à la carte bancaire qui consiste à récupérer de manière frauduleuse les données des cartes bancaires à partir d'un dispositif spécial inséré dans les distributeurs de billets de banques, puis à utiliser ces données pour dupliquer les cartes des victimes et débiter leurs comptes, et c'est 1% de la cybercriminalité au Cameroun selon l'ANTIC.

d'identité sur les réseaux sociaux[26], les simswap[27], les simbox[28].

Il existe cependant dans ce pays d'autres techniques non énoncées dans cette notice de l'ANTIC, à l'instar de l'ouverture de comptes avec de fausses identités, le vol des données des cartes bancaires, le vol des données des comptes virtuels, les fausses loteries, le defacement des données encore appelé webdefacement qui est une sorte de détournement de site, les redirections d'adresses IP à l'insu de l'internaute, ainsi que le chantage sur des entreprises dont on a au préalable bloqué les données.

B - LES HOAX

Communément appelés «Fake-news», il s'agit d'une véritable gangrène qui connait une croissance exponentielle. Ils sont utilisés à des fins politiques, sociales, économiques, culturelles, religieuses, d'hégémonie et autres par des individus malintentionnés pour manipuler l'opinion ou orchestrer des campagnes de propagande. Nul n'est épargné, même pas le Chef de l'Etat que les réseaux sociaux ont annoncé mort à de très nombreuses reprises.

La sanction de ce type d'infraction est essentiellement traitée dans le cadre du code pénal, ce qui n'est pas le cas des atteintes aux systèmes d'information qui sont particulièrement traitées dans un texte exclusivement dédié à la lutte contre la cybercriminalité et la promotion de la cybersécurité à savoir la loi du 21 décembre 2010.

2 - LES ATTEINTES AUX SYSTÈMES D'INFORMATION OU CYBERATTAQUES

Ce sont des attaques qui visent souvent des institutionnels comme les Etats, les entreprises, les organisations. On s'attaque aux systèmes d'information de

[26] Ce sont souvent les identités de hautes personnalités qui sont usurpées. Les cybercriminels le font pour extorquer de l'argent aux victimes en leur promettant emplois et marchés publics entre autres.

[27] Technique consistant à exploiter les défaillances dans le processus d'identification et de reconduction des cartes SIM auprès des opérateurs de téléphonie mobile pour s'approprier le numéro des victimes, émettre et recevoir des communications et en débiter les comptes d'argent.

[28] Ils consistent en l'utilisation d'un boitier électronique(SIMBOX) et du réseau internet afin de contourner les passerelles des échanges internationaux dans l'acheminement des communications téléphoniques internationales, afin de faire passer le trafic téléphonique international pour du trafic national et bénéficier de sa souplesse des tarifs.

ces institutionnels qui sont un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information. Une cyberattaque est «une action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support»[29]. Elles sont souvent ponctuelles, mais elles peuvent aussi s'inscrire dans la durée et être de ce fait évolutives et capables de s'adapter aux mesures défensives qu'on leur oppose.

Ce type d'actions nécessite une très haute connaissance de l'outil informatique. Dans sa loi du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, ce pays a pris en compte ce type d'atteintes dans ses articles 65, 66 et 68[30]. Le Cameroun a dans son histoire déjà enregistré des cyberattaques[31]. Tout comme les atteintes aux systèmes d'information, les atteintes aux personnes ont également été prises en compte et sanctionnées à maints égards.

3 - LES ATTEINTES AUX PERSONNES

Elles sont de plusieurs ordres.

A - LES ATTEINTES AUX DONNÉES À CARACTÈRE PERSONNEL

De manière générale, l'importance des données à caractère personnel semble encore échapper à la majorité des citoyens camerounais. On ne saurait les blâmer outre mesure, car la loi de 2010 sur la Cybersécurité et la lutte contre la cybercriminalité n'a pas abordée la question des données à caractère

[29] France, Défense Nationale, «Glossaire interarmées de terminologie opérationnelle», PIA-7.2.6.3_GIAT(2012), no 001/DEF/CICDE/NP

[30] L'article 65 érige en infraction l'accès frauduleux dans un système de traitement automatisé de données.

L'article 66 pour sa part sanctionne l'introduction frauduleuse de données et la falsification ou la suppression frauduleuse de données. Quant à l'article 68, il punit l'entrave au fonctionnement du système.

[31] Voire article agenceecofin.com op.cit.A titre d'esemple, on y apprend que , dans un rapport présenté en novembre 2011 par le ministre des postes et télécommunications qui faisait état de quelques données sur la cybercriminalité au Cameroun, ce responsable gouvernemental indiquait qu'entre 2008 et 2011, les sites de grandes institutions ont été piratés, à l'instar de ceux de la douane, du ministère des domaines et des affaires foncières (2008), de l'université de Yaoundé I, des quotidiens La nouvelle expression (2009), Cameroun Tribune (2011), du parti des démocrates camerounais (2011), sans oublier les sites officiels des personnalités comme celui du premier ministre également piraté

personnel qui n'y sont même pas définis ni évoqués.

En effet, les données à caractère personnel sont «des informations se rapportant à une personne vivante identifiée ou identifiable. Différentes informations dont le regroupement permet d'identifier une personne en particulier, constituent également des données à caractère personnel»[32]. Bien que tenus de les sécuriser et d'en assurer la confidentialité, les personnes chargées de collecter et de traiter les données personnelles sont souvent surpassées soit par les logiciels espions qui sont introduits dans leurs terminaux à leur insu par des personnes malveillantes qui en collectent des informations personnelles, soit par les cookies qui sont plutôt installés dans les disques durs de l'internaute par le gestionnaire des sites afin d'en collecter les informations personnelles pour une exploitation souvent commerciale et publicitaire.

L'article 65 de la loi sur la cybersécurité et la cybercriminalité sanctionne néanmoins aussi les atteintes aux données à caractère personnel. La même loi traite ailleurs des atteintes aux droits de la personnalité.

B - LES ATTEINTES AUX DROITS DE LA PERSONNALITÉ

Trois principaux droits de la personnalité sont visés ici;

1-) LE DROIT AU RESPECT DE LA VIE PRIVÉE

Il est fermement réaffirmé par l'article 41 de la loi No 2010/012 du 21 décembre 2010 en ces termes: «Toute personne a droit au respect de sa vie privée. Les juges peuvent prendre les mesures conservatoires, notamment le séquestre et la saisie pour empêcher ou faire cesser une atteinte à la vie privée».

La violation de la vie privée est sanctionnée entre autres par l'article 74 alinéa 1 et 84 alinéa 2 de cette loi de 2010 sur la cybersécurité et la cybercriminalité. Ces deux articles connaissent du fait de porter atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant sans l'autorisation de l'auteur les données électroniques ayant un caractère confidentiel, pour le premier, et de l'interception non autorisée, le

[32] https://ec.europa.eu»law»reform

détournement, l'utilisation ou la divulgation des communications électroniques émises ou reçues ainsi que l'installation d'appareils destinés à réaliser des interceptions , pour le second.

Dans la même veine, les articles 80 et 81 alinéas 1 de la loi N° 2010/013 du 21décembre 2010 régissant les communications électroniques au Cameroun sont également dédiées à la protection de la vie privée. Ces deux derniers articles traitent respectivement de la violation du secret des correspondances et utilisation, divulgation ou publication non autorisée du contenu d'une correspondance privée, d'une part, et de l'interception volontaire ou involontaire et la divulgation d'une correspondance privée au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre. L'article 81 alinéas 2 de cette loi pose les exceptions à ces sanctions.

Dans le même sens, la constitution camerounaise du 18 janvier 1996 révisée le 14 avril 2008 garantit en son préambule et en son article 44 le secret des correspondances contre les écoutes téléphoniques et l'interception des courriers ou des mails.

2-) LE DROIT À L'IMAGE;

Le droit d'une personne sur son image étant protégé au même titre que le droit sur la voix, toute personne célèbre ou anonyme peut s'opposer à l'utilisation sans autorisation de son image, quel que soit le lieu où elle se trouvait au moment où elle a été photographiée ou filmée, qu'il soit public ou privé. La violation de ce droit est sanctionnée par l'article 75 de la loi de 2010 sur la cybercriminalité et la cybersécurité.

3-) LE RESPECT DE LA VIE PRIVÉE DES SALARIÉS;

La législation camerounaise demeure muette sur la question, pourtant avec la généralisation de l'utilisation de l'informatique dans les postes de travail, de nombreux employeurs ont fait intrusion dans la vie privée des salariés à laquelle ils ont accès à travers le contenu de leurs ordinateurs qu'ils peuvent parfois contrôler à distance. Il est donc plus qu'impératif que des gardes fous soient mis en place dans ces relations professionnelles afin de protéger la vie privée des salariés.

Dans l'utilisation malveillante de l'internet pour atteindre les personnes, certains individus vont encore plus loin, au point de voler carrément l'identité de leur victime.

C - L'USURPATION D'IDENTITÉ

Cette pratique encore peu répandue sous nos cieux a des conséquences dramatiques en occident où les victimes sont dans la même situation que le néant, car dès qu'on vous vole votre identité, vous n'existez plus. La procédure pour se faire rétablir dans son identité est dès lors longue et onéreuse. Du fait de son caractère encore limité au Cameroun, le législateur n'a pas encore planché sur les usurpations d'identité par voie cybernétique. Il y a pourtant lieu de le faire au plus tôt, car les dispositions du code pénal qui traitent de l'usurpation de fonctions[33] ou de l'usurpation d'un titre[34] ne permettent pas de couvrir toute la complexité inhérente à l'usurpation d'identité. En effet, il s'agit dans ce dernier cas de la pratique par laquelle une personne utilise ou exploite sciemment les informations personnelles d'une autre personne à des fins illégales. En réalité, on utilise ici l'identité d'un tiers comme si on était ce tiers et on fait usage au profit de l'usurpateur des données pouvant permettre d'identifier le tiers. La traite des êtres humains via internet n'est pas moins grave.

D - LA TRAITE DES ÊTRES HUMAINS VIA INTERNET

Bien que de nombreux camerounais en aient été victimes via des réseaux d'immigration clandestine, la législation camerounaise ne semble pas encore avoir pris la mesure de la dangerosité et de l'inadmissibilité de cette pratique du point de vue de l'humain. En effet, la traite des êtres humains qui est assimilable à de l'esclavage moderne est une forme de criminalité organisée qui rapporte très gros aux criminels. Par la tromperie ou la contrainte, les victimes sont emmenées d'un pays ou d'une région au sens de continent pour un autre. La pédocriminalité est tout aussi moralement intolérable.

[33] Article 216 du code pénal camerounais
[34] Articles 219 et 220 du code pénal camerounais

E - LA PÉDOCRIMINALITÉ OU ATTEINTE AUX MINEURS

Dans la majorité des cas, il s'agit d'une criminalité «locale» qui est traitée par le code pénal, les infractions étant souvent commises par la proximité des victimes. Toutefois, cette infraction prend de plus en plus une dimension internationale que le législateur n'a pas encore pris en compte. Il s'agit ici des cas où les actes pédocriminels s'insèrent dans la logique de bandes criminelles internationales qui commettent leurs infractions au moyen d'internet, ou lorsqu'il s'agit des délinquants sexuels itinérants.

A côté de ces atteintes aux personnes à la gravité reconnue, se trouve d'autres types d'actes cybercriminels, à l'instar des délits de presse.

4 - LES DÉLITS DE PRESSE

Le réseau internet est assimilé à un moyen de communication audiovisuel et est à ce titre soumis aux dispositions de la loi N° 90/052 du 19 décembre 1990 relative à la liberté de communication sociale, modifiée par la loi N° 96/04 du 4 janvier 1996 ainsi que le décret No 2000/158 du 3 avril 2000 fixant les conditions et les modalités de création et d'exploitation des entreprises privées de communication audiovisuelle.

Tirant les conclusions de ce qui précède, on comprend que si le principe de la liberté d'expression est de règle sur internet, on peut néanmoins être sanctionné pour diffamation, injure, propagation de fausses nouvelles, incitation à la haine dont traite l'article 77 de la loi de 2010 sur la cybersécurité et la cybercriminalité.

Par ailleurs, en cas de promotion du terrorisme via internet et en vertu des dispositions de la loi No 2014/028 du 23 décembre 2014 notamment en son article 8, on peut être poursuivi pour des écrits promouvant le terrorisme ou en faisant l'apologie. Dans ce cas, on est poursuivi par les juridictions militaires.

Les atteintes à la propriété intellectuelle peuvent être faites par voie cybernétique.

5 - LES ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE

L'une des atteintes les plus communes ici ce sont les contrefaçons qui peuvent se libeller en termes de criminalité pharmaceutique, piratage des logiciels, téléchargement illégal de la musique, des films ou des livres sur internet. Dans tous les cas, ces actes sont des violations des droits de la propriété intellectuelle qui se subdivise en deux catégories.

Le droit de la propriété littéraire et artistique qui est la première catégorie ici comprend le droit d'auteur et les droits voisins du droit d'auteur. Il est régi par la loi No 2000/11 du 19 décembre 2000 relative aux droits d'auteurs et aux droits voisins, laquelle vise à protéger les auteurs, les artistes interprètes, les producteurs de phonogrammes et de vidéogrammes et les entreprises de communication audiovisuelle.

Pour sa part, la seconde catégorie qui porte sur les droits de la propriété industrielle comporte les brevets d'invention, les marques de produits ou de services, les dessins ou modèles industriels, les indications géographiques, les obtentions végétales et les produits semi conducteurs, toutes choses qui peuvent être volées à travers internet. Au Cameroun, les dispositions applicables dans ce cadre sont celles de l'accord de Bangui du 2 mars 1977 révisé le 24 février 1999 instituant l'organisation africaine de la propriété intellectuelle.

Bien évidemment, les textes, même les plus pertinents ne servent à rien s'il n'y a pas une bonne architecture institutionnelle pour les mettre en œuvre.

II - DES MECANISMES INSTITUTIONNELS EN CONSTRUCTION

Construite autour d'institutions diverses tant dans leur organisation, leurs missions que la typologie des moyens dont ils disposent, le dispositif institutionnel au Cameroun pour lutter contre la cybercriminalité est très simple, car il est composé principalement de trois groupes d'organisations à savoir, celles qui mènent les enquêtes et réunissent les preuves d'actes cybercriminels pour transmission aux juridictions, celles qui les assistent par leur technicité

dans cette mission de recherche et de constatation des infractions cybercriminelles, et enfin les juridictions en charge du jugement des cybercriminels. Aussi, pouvons-nous les regrouper en organes de recherche et de constatation d'infractions cybercriminelles (A), d'une part, et en organes juridictionnels (B), d'autre part.

A - LES ORGANES DE RECHERCHE ET DE CONSTATION DES INFRACTIONS CYBERCRIMINELLES AU CAMEROUN

On peut distinguer ici les organes d'enquête (1) des organes administratifs et techniques (2)

1 - LES ORGANES D'ENQUÊTE

Bien que diversifiés dans leur typologie, ils exercent leurs missions (a) avec les atouts et les limites qui sont les leurs (b).

A - MISSIONS ET TYPOLOGIE

Les organes d'enquête sont en charge de rechercher, de constater les infractions cybercriminelles, d'en réunir les preuves et de les présenter aux instances en charge du jugement. Il n'y a là en somme rien d'extraordinaire, car il s'agit là de la mission traditionnelle des officiers de police judiciaire qui font exactement la même chose que pour la criminalité traditionnelle. C'est donc dire que comme pour cette criminalité dite traditionnelle, et hormis les cas d'officiers de police judiciaire à compétence spéciale expressément créés par des textes spécifiques, ce sont les unités traditionnelles de la police, de la gendarmerie et dans une certaine mesure de le DGRE[35] qui sont en charge de cette mission. A ces institutions nationales, on peut joindre Interpol[36] sur le plan international qui peut agir ici dans le cadre de ses pouvoirs conventionnels. En effet, au Cameroun, ce ne sont essentiellement que ces institutions qui peuvent

[35] Direction Générale de la Recherche Extérieure.

[36] Cette organisation a conçu et appliqué par exemple sa «stratégie en matière de lutte contre la cybercriminalité». L'intervention d'une structure comme Interpol souligne l'importance de la coopération policière en matière de lutte contre la cybercriminalité car ce sont souvent des infractions sur plusieurs Etats.

présenter les cybercriminels à la justice camerounaise. Elles ont bien évidemment des forces et des faiblesses.

B - FORCES ET FAIBLESSES

Les principales forces de ces structures d'enquête sont: leur expérience cumulée en matière d'enquêtes, le soutien très important de l'appareil administratif sur lequel elles s'appuient, leur réseau d'informateurs et leur maillage territorial.

Leur principale faiblesse réside dans le fait que ni à la police, ni à la gendarmerie, il n'y a eu création d'unités dédiées spécialement à la lutte contre la cybercriminalité avec la formation et les moyens appropriés, un peu comme on l'a fait à la police pour répondre à certaines menaces en créant une compagnie de sécurisation des diplomates ou une compagnie de sécurisation des établissements scolaires au sein du CCGMI[37]. On s'est plutôt contenté d'ajouter le portefeuille de la lutte contre la cybercriminalité aux vieilles unités déjà existantes comme la direction de la police judiciaire, sans forcément lui donner les moyens techniques et humains nécessaires pour relever ce défi. Il y a donc souvent un déficit d'expertise.

2 - LES ORGANES ADMINISTRATIFS ET TECHNIQUES

Bien que divers, ils ont une mission commune dans le cadre de la lutte contre la cybercriminalité (a) qu'ils accomplissent avec leurs atouts et leurs faiblesses(b).

A - MISSION ET TYPOLOGIE

Ils ont deux principaux ordres de mission dans la lutte contre la cybercriminalité. En effet, dans le cadre des poursuites pénales, ils ont pour mission d'assister les OPJ de la police, de la gendarmerie et de la DGRE dans leur mission de recherche et de constatation des infractions cybercriminelles et d'assemblage des preuves. Dans ce sens, ce sont ces organes à l'instar de l'ANTIC qui réunissent les preuves numériques et autres preuves dont l'extraction exige certains équipements et certaines compétences techniques et

[37] Commandement Central des Groupements Mobiles d'Intervention de la Police.

technologiques dont les OPJ ne disposent pas toujours.

Dans le cadre administratif, ces organes recherchent et constatent les infractions cybercriminelles, en réunissent les preuves, non pas pour les remettre aux OPJ, mais plutôt pour les utiliser dans le cadre des procédures administratives contre les contrevenants et les sanctionner. C'est dire que dans ce cadre, ces organes administratifs se positionnent en instances de jugement sur des considérations purement administratives. C'est le cas par exemple avec le conseil national de la communication[38]. Toutefois, rien n'empêche que pour les mêmes faits, l'OPJ connaisse en même temps des aspects d'ordre pénal.

Pour ce qui est de leur typologie, on retrouve des organes divers à savoir tant les ministères que les agences, les conseils et autres[39].

B - FORCES ET FAIBLESSES

Leur principale force réside dans leur expertise et leurs faiblesses dans l'insuffisance des moyens techniques et technologiques d'investigation, et parfois leur obsolescence au regard des avancées fulgurantes de la technologie et de l'usage dont en font les cybercriminels.

Par ailleurs, la faiblesse majeure ici réside dans l'insuffisance de la coordination des structures en charge de la lutte contre la cybercriminalité. En effet, il existe de très nombreux intervenants au Cameroun en matière de lutte contre la cybercriminalité, mais il n'existe ni des canaux suffisants d'interconnexion, de communication, de collaboration, ni de structure centrale de coordination.

Toutefois, leur travail et les preuves techniques fournies sont d'une aide

[38] https://www.cameroon-tribune.cm» …Dans sa cession récente du 18 mars 2022 par exemple, le CNC a infligé des avertissements à l'endroit des directeurs de publication et une suspension d'exercice de la fonction pour une duréée de deux pour un journaliste de la chaine vision 4.

[39] A titre d'exemple, nous avons le Ministère des Postes et Télécommunications, chargé de l'élaboration et du suivi de la mise en œuvre de la politique nationale en matière de sécurité des communications électroniques et des systèmes d'information: de l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC), qui assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des réseaux de communications électroniques: du Conseil National de la Communication (CNC) qui régule les activités des médias audiovisuels: de l'Agence de Régulation des Télécommunications (ART) qui assure pour le compte de l'Etat la régulation, le contrôle et le suivi des activités des opérateurs, des exploitants des réseaux et des fournisseurs de services de communications électroniques: du Conseil National de la Publicité (CNP) qui assiste et conseille l'Etat, notamment le ministère de la communication dans sa mission de régulation du secteur de la publicité.

précieuse pour les organes juridictionnels de lutte contre la cybercriminalité au Cameroun.

B - LES ORGANES JURIDICTIONNELS DE LUTTE CONTRE LA CYBERCRIMINALITE AU CAMEROUN

Il s'agit de l'instance de jugement, celle qui sur la base des textes ci-dessus confirme, infirme ou requalifie l'incrimination proposée par les organes de recherche et de constatation, puis arrête la sanction retenue au regard des éléments dont il dispose. Bien évidemment, nous sommes ici purement dans la procédure judiciaire et non dans la procédure administrative. Cette instance judiciaire peut travailler soit en situation d'autosuffisance (1), soit en situation de dépendance extérieure, lorsqu'elle a besoin de la coopération judiciaire (2).

1 - L'INSTANCE JUDICIAIRE EN SITUATION D'AUTOSUFFISANCE

Il s'agit essentiellement des cas où tous les éléments matériels de l'infraction interviennent dans le territoire camerounais. L'instance judiciaire n'a donc, ici, aucune autre complication que les contraintes domestiques inhérentes à la mission qui consiste à rendre justice au Cameroun. Il n'est donc pas besoin, dans ce cadre, de faire appel à l'aide judiciaire extérieure. On peut toutefois, recourir à l'aide technique extérieure, mais il s'agit essentiellement, des experts, comme on en utilise dans toutes les procédures traditionnelles au Cameroun. L'instance judiciaire dont il est question, ici, n'est pas seulement les tribunaux d'instance, mais il s'agit de tous les éléments susceptibles de dire le droit dans une affaire cybercriminelle, y compris la cour d'appel. Bien évidemment, dans une telle configuration, les organes juridictionnels disposent d'atouts importants (a), mais ils sont aussi plombés par des limites qu'il s'agit de surpasser (b).

A - ATOUTS

Les atouts dans ce cadre, sont quasiment les mêmes que ceux des organes d'enquête à savoir l'expérience, l'apport ou le soutien de l'appareil administratif et l'autorité inhérente à leur fonction.

B - INSUFFISANCES

La plus grande insuffisance de l'instance judiciaire camerounaise est le manque d'expertise, car faute de formation, de nombreux magistrats sur le terrain n'ont pas une bonne connaissance des questions cybercriminelles. Il manque aussi de coordination dans le traitement judiciaire des questions cybercriminelles et l'absence de pratique judiciaire avec une jurisprudence étoffée n'aide pas.

2 - L'INSTANCE JUDICIAIRE EN SITUATION DE DÉPENDANCE EXTÉRIEURE: LA COOPÉRATION JUDICIAIRE

Comme déjà souligné, la cybercriminalité est un type de criminalité qui implique souvent beaucoup d'éléments d'extranéité. Aussi, la probabilité pour que les instances juridictionnelles camerounaises aient recours à celles des pays étrangers est plus grande ici que dans tout autre domaine. Se pose dès lors la question de la coopération judiciaire qui elle-même représente un casse-tête important pour les instances de jugement des pays du sud. En effet, la coopération judiciaire se heurte souvent aux principes internationaux de souveraineté et de protection des nationaux. Elle est donc souvent soumise au préalable de la signature d'un accord en amont entre Etats. Or, on constate que les pays du Nord rechignent à signer de tels accords avec ceux du Sud. C'est donc dire que pour des considérations de non fluidité de la coopération judiciaire avec l'extérieur, beaucoup de procédures de jugement dans des affaires de cybercriminalité peuvent être bloquées. C'est conscient de ces difficultés que sur un plan sous régional tout au moins, les chefs d'Etats et de gouvernement de la CEMAC ont signé un accord de coopération judiciaire[40] et un autre de coopération policière[41].

On le voit donc, les développements qui précèdent traitent déjà des forces et faiblesses de la procédure de jugement en situation de dépendance extérieure, puisqu'il apparaît que la coopération qui existe avec l'extérieur proche est quasi

[40] Op.cit
[41] Op.cit.

inexistante avec l'extérieur éloigné, composé des pays d'Afrique autres que ceux de la CEMAC et des pays des autres continents. En effet, il n'existe que très peu ou pas d'accord de coopération judiciaire entre le Cameroun et les autres pays d'Afrique hors CEMAC, situation surprenante pour une même région.

CONCLUSION

Le dispositif camerounais de lutte contre la cybercriminalité semble au final connaître de belles avancées au regard des efforts normatifs, institutionnels et même infrastructurels déployés. S'agissant de ce dernier point, des efforts plus importants s'imposent pour doter le Cameroun de l'infrastructure technologique et technique nécessaire pour affronter des cybercriminels qui semblent toujours plus en phase avec les évolutions techniques et technologiques que les Etats, individus et institutions victimes. Pour ce qui est des considérations textuelles et institutionnelles de la lutte contre la cybercriminalité au Cameroun, quelques recommandations peuvent être tirées des différents développements ci-dessus:

- la création ou la désignation formelle d'un organe en charge de la coordination de la lutte contre la cybercriminalité. On pourrait dans ce sens désigner un ministère ou même créer une autorité nationale de lutte contre la cybercriminalité;
- la multiplication des efforts diplomatiques pour obtenir partout en Afrique et au-delà des accords de coopération judiciaire et même policière dans la lutte contre la cybercriminalité;
- la ratification rapide des conventions de Budapest et de Malabo sur la cybercriminalité, ainsi que de tous les textes internationaux susceptibles d'apporter au Cameroun une plus-value en matière de lutte contre la cybercriminalité;
- la multiplication dans ce pays des sessions de formation des différents intervenants de la lutte contre la cybercriminalité: magistrats, OPJ, gardiens de prisons, etc;

- l'intégration de modules sur la lutte contre la cybercriminalité dans la formation initiale de ces différents intervenants;
- le recours aux experts dans le processus de jugement pour une justice efficace[42];
- l'élaboration et la mise en œuvre d'une politique de formation ou de mise en place d'un matelas local de compétences en informatique et numérique de haut vol comme l'ont fait des pays tels que l'Inde, la Russie ou la Chine, lesquels réussissent par ces compétences à contourner les blocages éventuels des GAFAM face aux volontés internes de lutte contre certains types de cybercriminalité;
- la poursuite de l'élaboration d'une stratégie gouvernementale et de stratégies sectorielles de cybersécurité[43].

REFERENCES BIBLIOGRAPHIQUES

ARTICLES

1 B. Louis-Sidney, «La dimension juridique du cyberespace», *Revue internationale et stratégique 2012/3 (No87), pp73-81.*

DOCUMENTS NORMATIFS

2 Textes internationaux
3 Convention de Budapest sur la cybercriminalité, adoptée en Hongrie le 23 Novembre 2001
4 Convention de l'Union Africaine sur la Cyber sécurité et la protection des données, adoptée à Malabo le 23 juin 2014.
5 la Déclaration universelle des droits de l'Homme du10 décembre 1948 à Paris
6 Pacte international relatif aux droits civils et politiques du 16 décembre 1966 à New york
7 Convention de l'Union Internationale des Télécommunications du 22 décembre 1992 à Genève
8 Constitution de l'Union Internationale des Télécommunications du 22 décembre 1992 à Genève
9 Règlements des radiocommunications de 2007

[42] Il est admis d'ailleurs par le code de procédure pénale dans ses articles 203 à 217.
[43] Il s'agit là d'un projet entamé mais non abouti du gouvernement camerounais.

10 Convention sur l'emploi de la radiodiffusion dans l'intérêt de la paix de 1936
11 Convention de Montego Bay de 1982
12 Convention internationale relative à la protection des câbles sous-marins de 1884
13 Traité de l'espace de 1967

TEXTES INTERNES

14 Loi N° 96/06 du 18 janvier 1996, portant révision de la constitution du 2 juin 1972, modifiée et complétée par la loi No 2008/001 du 14 avril 2008
15 Loi N° 90/052 u 19 décembre 1990 relative à la liberté de communication sociale, modifiée par la loi No 96/04 du 4 janvier 1996
16 Loi N° 2000/11 du 19 décembre 2000 relative aux droits d'auteurs et aux droits voisins
17 Loi n° 2005/007 du 27 juillet 2005 portant code de procédure pénale qui organise la poursuite des infractions en matière de cybercriminalité
18 Loi N° 2006/018 du 29 décembre 2006 régissant la publicité au Cameroun
19 Loi N° 2010/012 du 21 décembre 2010 relative à la cyber sécurité et à la cybercriminalité au Cameroun
20 Loi N° 2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, modifiée et complétée par la loi N°2015/006 du 20 avril 2015
21 Loi N° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun
22 Loi No 2014/028 du 23 décembre 2014 portant répression des actes de terrorisme
23 Loi N° 2015/006 du 20 avril 2015 régissant l'activité Audiovisuelle au Cameroun.
24 Loi N° 2016-7 du 12 juillet 2016 portant code pénal, qui fixe certaines peines en matière de cybercriminalité
25 Loi N° 2017/012 du 12 juillet 2017 portant code de justice militaire
26 Décret N° 2000/158 du 3 avril 2000 fixant les conditions et les modalités de création et d'exploitation des entreprises privées de communication audiovisuelle
27 Décret N° 2013/0404/PM du premier ministre du 27 février 2013 précisant les modalités de gestion des ressources de nommage et d'adressage (sur internet au Cameroun)

RAPPORTS

28 https://www.dictionnaire-juridique.com/definition/ntic-nouvelles-technologies-de-l-inf... Consulté le 21 avril 2022 à 22H22'.
29 https://www.agenceecofin.com/?option=com_k&2id=3266&view=item&itemid=181&tmpl=c... Consulté le 21 avril 2022 à 1h 20'.
30 https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf
31 https://www.ACCENTURE.COM/FR-FR/INSIGHT-COST-OF-CYBERCRIME-2017.
32 France, Défense Nationale, «Glossaire interarmées de terminologie opérationnelle», PIA-7.2.6.3_GIAT(2012), no 001/DEF/CICDE/NP

33 https://ec.europa.eu»law»reform
34 Notice ANTIC sur les actions menées par cette institution pour renforcer la cybersécurité et lutter contre la cybercriminalité
35 Site internet investir au Cameroun, 3 mars 2016
36 Projet sectoriel de stratégie de lutte contre la cybercriminalité de la DGSN de 2017
37 https://www.larousse.fr»français, consulté le 19 avril 2022 à 22h40'.

L'IMPERATIF DE LA MUTUALISATION ET DE LA COORDINATION DES MECANISMES DE LUTTE CONTRE LA PROPAGATION DE COMPORTEMENTS A RISQUE A TRAVERS INTERNET ET LES MEDIA SOCIAUX

Alain KENMOGNE
Agrégé des Facultés de Droit
Professeur Titulaire CAMES
Chef du département de droit des affaires et de l'entreprise, Université de Yaoundé II, Soa

INTRODUCTION

L'avènement des Nouvelles Technologies de l'Information et de la Communication (N.T.I.C.)[1], constitue à de nombreux égards, une révolution sans précédent, que certains n'hésitent pas à comparer à la révolution industrielle du XIX^{ème} siècle[2]. En effet, avec le développement du traitement

*L'auteur voudrait témoigner sa gratitude au Docteur F., Nguelé Mballa dont la contribution à la production de cette réflexion a été inestimable.

[1] L'acronyme N.T.I.C. est utilisé dans la présente étude pour désigner les Nouvelles Techniques de l'Information et de la Communication qui se sont développées au cours des dernières décennies. D'un point de vue définitionnel, il s'agit des technologies de l'informatique, de l'audiovisuel, des multimédias, de l'Internet et des communications qui permettent aux utilisateurs, de communiquer, de stocker, de manipuler, de produire et de transmettre l'information sous toutes les formes. L'on doit donc y englober l'ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des communications, qui ont permis l'émergence des moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information. Dans ce sens on peut lire M., Ndoumga, Les Technologies de l'Information et de la Communication: Vers une mise à jour des conditions de formation du contrat ?, International Multilingual Journal of Science and Technology Vol. 5, Mai-2020, pp.1026 et suivants.

[2] I., De Lamberterie, L'écrit dans la société de l'information, *Mélanges Denis Tallon, d'ici, d'ailleurs: harmonisation et dynamique du droit*, 1999, p. 120. et même P-M. Reverdy, La matière pénale à l'épreuve des nouvelles technologies, Thèse de Doctorat, Université Toulouse I, 2005, p. 79 et s.

automatique des données[3], et leur circulation ultra rapide et au-delà de toute frontière par le biais des nouveaux canaux de télécommunication, il est apparu plus qu'impératif de considérer à côté de la société réelle, un cadre sociétal sans cesse dématérialisé, qui constitue pour ainsi dire la matrice des relations humaines aujourd'hui. Les manifestations les plus perceptibles de ce phénomène se donnent à voir notamment au travers de l'émergence des média sociaux et de l'internet. Le vocable «média sociaux», également dénommé «réseaux sociaux» dans le langage courant, recouvre des espaces virtuels qui font usage des N.T.I.C., et permettent une interaction sociale à distance entre des individus ou groupes d'individus, lesquels peuvent ainsi créer et partager des contenus digitaux, voire contracter et commercer via des terminaux divers (téléphone, ordinateur, tablette…etc.). On doit en fait y comprendre un groupe d'applications en ligne et de programmes informatiques, réalisant des communautés sociales virtuelles d'échange de données générées par des utilisateurs, et procédant grâce à la technologie de l'internet. Par internet justement, il faut entendre le plus grand réseau d'interconnexion numérique des terminaux informatiques de la planète, qui aujourd'hui, de par son expansion dans tous les coins du globe, s'est érigé en cadre d'émergence d'un véritable «village virtuel global» et d'un type nouveau de société, entretenue par de multiples média sociaux en ligne[4].

Ce nouvel ordre social, généré et imposé par cette révolution de l'internet et de plus en plus, épuré de toute frontière territoriale, ne manque pas de susciter des questionnements quant à sa régulation par les disciplines juridiques. Le dessein est alors de lutter contre l'instauration ici d'un état de nature «rousseaunien», notamment par la lutte contre la prolifération des agissements portant atteinte à certains idéaux, valeurs sociales et biens juridiques[5] au sein de ce cadre social dématérialisé. Dans cette perspective,

[3] Les «données» désignent les informations créées et utilisées par le biais d'un programme informatique, ou qui se prêtent à un système de traitement automatisé de l'information. Cf. B., Pereira, la lutte contre la cybercriminalité: de l'abondance de la norme à sa perfectibilité, *Revue Internationale de Droit Économique*, 2016, p.388.

[4] Le terme «internet» a été formé à partir de l'anglais «INTERconnected NETworks» équivalant à «réseaux interconnectés». Cf. PH. Le Tourneau, *Contrats informatiques et électroniques*, 7ème éd., Paris, Dalloz Référence, 2013, p. 3. Le réseau internet regroupe en fait une multitude de réseaux régionaux, gouvernementaux et commerciaux…etc. On parle à propos du «réseau des réseaux». Sur ces points voir K. Hafner, *Where wizards stay up late: The origins of the internet*, New York, Touchstone, 1996, p. 12: J. Naughton, *A brief history of the future: from radio days to internet years in a lifetime,* New York , WoodStock, 1999, p. 140.

[5] Sur la notion de «biens juridiques«, il convient de noter qu'elle demeure une question fondamentale en droit. D'après les

il faut observer que la prolifération de comportements déviants à travers internet et les média sociaux a déjà donné lieu à un développement normatif non négligeable par des textes adressant, directement ou indirectement, la question de cybercriminalité et de la cybersécurité[6]. Seulement, il importe de noter que l'une des caractéristiques de cette cybercriminalité sans cesse grandissante est que d'un point de vue technique, les agissements déviants se créent et se mutent ici presque quotidiennement au gré de l'évolution technologique, et de ce fait passent pour être difficilement saisissables par le droit positif[7]. De même, et spécialement sur le terrain pénal, on doit regretter la disparité de l'appellation et de la considération pénale de ses agissements selon les ordres juridiques nationaux[8], tout autant que les difficultés inhérentes à l'identification et au dégagement des responsabilités pénales de leurs auteurs et ou complices, eu égard à la transnationalité de la commission des actes ici visé, conséquence elle-même des caractéristiques de l'univers cybernétique[9]. Aussi, face à ces difficultés et d'autres qui rendent complexe la saisine de ce type de délinquance par les seuls ordres juridiques nationaux, se pose, non pas la question de savoir s'il faut lutter contre cette forme de criminalité[10], mais celle de savoir comment le faire.

---

auteurs, il s'agit, à travers elle, de déterminer les critères à partir desquels la norme notamment pénale transforme les intérêts sociaux en valeurs dignes de protection juridique. Sur cette question voir M. Fabre-Magnan, La dignité en droit: un axiome, *R.I.E.J*., 2007, n°58, p. 2., A. Supiot, *Homo Juridicus, Essai sur la fonction anthropologique du Droit*, Paris, Seuil, collection «La couleur des idées», 2005, spécialement p. 37, tous cités par F. Nguele Mballa, La protection pénale du patrimoine immatérielle en droit camerounais: le cas des biens de la propriété intellectuelle, Thèse de Doctorat PhD en Droit Privé et Sciences Criminelles, Université de Yaoundé 2, 2019, p.4.

[6] On citera notamment dans ce sens les lois camerounaises N° 2010/012 du 21 décembre 2010 relative à la cyber sécurité et la cyber criminalité, et N° 2010/021 du 21 décembre 2010 régissant le commerce électronique.

[7] Notamment par le droit pénal. Du fait du principe de l'interprétation stricte, par exemple, un comportement peut ne pas rentrer dans les termes de la prévention. Ce qui, à défaut de susciter une remise en cause de certains grands principes de cette discipline, soulève au moins le problème de la manière de légiférer en la matière.

[8] Exemple, l'homosexualité qui est constitutive d'une infraction dans un ordre juridique comme celui camerounais peut ne pas l'être dans un autre, pareillement pour l'adultère …etc. Cette disparité ne manque pas d'avoir son reflet dans le monde cybernétique, cadre parallèle de facilitation de la commission de ses infractions.

[9] Cette délinquance recouvre en effet une dimension mondiale. La localisation des actes criminels suscite ici des débats houleux sur l'application de la territorialité pénale au cybercrime. Les actes criminels ici imposent souvent en fait que soient convoqués des acteurs de natures diverses, qu'il s'agisse des hébergeurs, des fournisseurs d'accès ou des internautes situés tous très généralement loin les uns des autres, et de bout en bout de la planète. Toute chose qui implique l'interpellation non sans mal de plus d'un ordre juridique pour l'identification non seulement de la norme applicable, mais aussi de la juridiction répressive compétente. Nous y reviendrons *infra*.

[10] Il n'y aurait aucune raison de ne pas lutter contre cette criminalité qui emprunte le moyen de l'internet. Au contraire, compte tenu de l'ampleur potentiellement plus grande, cette lutte devrait plutôt accentuée.

Sans méconnaitre les apports des divers mécanismes mis en œuvre par les Etats dans leurs systèmes juridiques respectifs afin d'instaurer un ordre public numérique[11], il y a lieu de déplorer que la majeure partie des réponses étatiques soient unilatérales et entreprises principalement dans les ordres internes, en dépit de quelques initiatives et approches globalisantes[12]. Or, ces réponses individuelles, en dehors de leur potentielle inefficacité, portent en elles le germe de suspicion de la part des autres pays. Aussi, en fait de réponse aux menaces sécuritaires sur la sphère cybernétique et dans une dynamique d'émancipation de l'état de nature sur internet et les médias sociaux, la présente réflexion vise à s'appesantir sur un postulat épistémologique de lutte contre la cybercriminalité, focalisée sur une dynamique mutualisante et coordonnée. Concrètement, et dans le dessein de proposer une approche permettant d'instaurer l'ordre public sur internet et les média sociaux, notre interrogation tourne autour de la question suivante: **n'est-il pas nécessaire de procéder à une mutualisation et une coordination des divers mécanismes étatiques de lutte contre la propagation de comportements à risque sur la sphère cybernétique ?** C'est dire que nous nous appesantissons ici non seulement sur les fondements de la préférence du recours à cette approche mutualisée et coordonnée, que sur la configuration normative qu'elle peut prendre du point de vue du droit, non sans évoquer les difficultés qui peuvent se présenter à son propos.

Bien que beaucoup d'écrits aient été consacrés à la problématique des mécanismes juridiques à mettre en œuvre pour la lutte contre la délinquance via les médias sociaux et internet[13], l'authenticité de la présente réflexion

[11] Nous empruntons cette expression à Ph., Mouron et C., Piccio, (sous la direction de), Introduction, *L'ordre public numérique*. *Liberté, propriété, identités*, P.U.A.M., 2015, p.21.

[12] Nous pouvons, dans ce sens, citer la convention européenne de Budapest sur la cybercriminalité du 23 novembre 2001, qui évoque des standards internationaux en matière de lutte contre la cybercriminalité. Dans le même sens nous pouvons mentionner la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractères personnel du 27 juin 2014.

[13] Cf. B.Pereira, La lutte contre la cybercriminalité: De l'abondance de la norme à sa perfectibilité, *Revue Internationale de Droit Économique*, *op.cit*., E. Stella. L'adaptation du droit pénal aux réseaux sociaux en ligne , Thèse de Doctorat en Droit Privé et Sciences Criminelles, Université de Lorraine, 2019, 485 p.: B. Stern, Vers la Mondialisation Juridique ? Les Lois Helms-Burton et d'Amato Kennedy, *R.G.D.I.P.*, Paris, 1996, pp. 979-1003: S. El Zein, L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie, *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, Lyon, Presse Universitaires de Lyon, 2001, pp. 153 et suivants.

tient essentiellement à ce qu'elle met l'accent sur la nécessité, et même l'urgence, d'une approche plurielle et d'une dynamique conjuguée en termes de coordination et de mutualisation des mécanismes de lutte contre la prolifération des agissements déviants sur les plateformes numériques. En guise d'hypothèse, le postulat est le suivant: face à la montée fulgurante de comportements déviants sur internet et les médias sociaux, le nécessaire et urgent recours à une dynamique conjuguée en termes de mutualisation et de coordination des mécanismes de lutte contre la prolifération des comportements à risque sur internet et les médias sociaux, trouve un fondement certain dans un argumentaire d'ordre à la fois philosophico-technologique et juridique. Aussi, envisageons-nous tour à tour les fondements de cet impératif de mutualisation et de coordination des mécanismes de lutte contre la prolifération des comportements déviants sur les média sociaux et internet (I) et la configuration possible de cette approche mutualisée et coordonnée (II).

I - LES FONDEMENTS DE LA NÉCESSITÉ D'UNE APPROCHE MUTUALISÉE ET COORDONNÉE

Ainsi que l'observe Olinet;

«*Espace virtuel qu'aucune frontière ne délimite, qu'aucun fleuve ne borne et qu'aucun pouvoir central ne régente, l'Internet est avant tout un nouvel espace d'expression humaine, un espace qui est celui de la liberté où chacun peut agir, s'instruire et s'exprimer. ….Extraterritorialité et rapidité des réseaux, fugacité et volatilité des données, anonymat, communication quasiment instantanée à un coût modéré, complexité croissante, le cyberespace est aussi un terrain de prédilection pour les délinquants: il réunit pratiquement tous les ingrédients pour réaliser le crime parfait !»*[14].

Le propos de ce spécialiste des questions de cybercriminalité exprime déjà l'idée forte selon laquelle le réseau internet, autant que les médias sociaux qu'il héberge, comporte déjà en lui-même les germes de sa propre

[14] M. Olinet, Cybercriminalité: énoncé du cas pratique et synthèse des réponses, *L'harmonisation des sanctions pénales en Europe*, (Sous la direction de M. Delmas-Marty, G. Giudicelli-Delage, E. Lambert-Abdelgawad), Paris, Société de Législation Comparé, 2003, p.1.

nocivité dans la prolifération des comportements déviants. Dans la criminogénèse de cette déviance, la doctrine s'accorde, en effet, à relever que les facteurs sont de divers ordres, notamment philosophico-technologique et juridico-normatif. Aussi, la diversité de ces facteurs interpelle-t-elle l'impératif d'une approche synergique intégrant tous les aspects de la question, de même que l'urgence d'une dynamique concertée. C'est dire qu'au crédit de la nécessaire implémentation d'une approche mutualisée et coordonnée de lutte contre la propagation de comportements à risque à travers internet et les médias sociaux, l'on peut raisonner de façon multisectorielle et, sans prétendre à l'exhaustivité, en partant d'arguments tenant tantôt de l'ordre des aspects philosophico - technologiques de l'internet et des média sociaux d'une part (A), et tantôt de l'ordre des aspects relevant des sciences juridiques d'autre part (B).

A - L'ARGUMENTAIRE D'ORDRE PHILOSOPHICO – TECHNOLOGIQUE DE LA NÉCESSITÉ D'UNE APPROCHE MUTUALISÉE ET COORDONNÉE

L'essentiel des arguments d'ordre philosophico – technologique qui participe à soutendre la nécessaire mutualisation et coordination requise des mécanismes de lutte contre la propagation des comportements déviants sur internet et les médias sociaux, trouve son creuset dans la philosophie maitresse de l'internet, laquelle entretient sa configuration technique. Ainsi, au cœur de la conception et de la réalisation de la révolution de l'internet et des Nouvelles Technologies de l'Information et de la Communication, se trouve l'idée de liberté et de célérité de circulation de l'information à l'échelle planétaire[15], et ce en dehors de toute restriction. En effet, au principe de la technologie de l'internet et des réseaux sociaux, se trouve l'argumentaire de la mise sur pied d'un procédé simple, facile d'accès, aisé d'usage, affranchie de restrictions, de faible coût d'exploitation, susceptible de permettre des interactions culturelles et des échanges ultra rapides d'informations dans un espace virtuel appelé le cyberespace[16]. Comme le souligne William Gibson,

[15] S. El Zein, L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie, *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, *op. cit*. p. 154.
[16] B., Stern Vers la Mondialisation Juridique ? Les lois Helms-Burton et d'Amato Kennedy, *R.G.D.I.P.*, pp. 979 et

la culture de l'internet se conçoit comme: «*Un dépassement des limites et tout particulièrement des frontières du corps et de la chair qui sont encombrants dans les voyages et dans la communication*»[17].

Ce dernier parle alors, à ce propos, de cyberespace pour décrire l'univers des N.T.I.C. et de l'internet, un univers issu de ce «réseau des réseaux», et conçu pour être dépourvu de toute barrière physique, de tout mur ou entrave à la circulation ultra rapide des informations. Dans cette perspective, ces technologies sont configurées sur la base des paradigmes de célérité, de simplicité d'accès à l'information tout autant que de traitement, de modification ou d'échange de celle-ci, de restriction au maximum des leviers, obstacles et barrières de toutes sortes et liées notamment au coût, à l'anonymat, à la territorialisation…etc.

Pour ainsi dire, le cyberespace comporte en lui-même et de par sa philosophie maitresse, beaucoup de caractéristiques qui prennent de l'importance lorsqu'on envisage la problématique de sa régulation. L'ensemble de ces caractères et propriétés qui particularisent l'environnement de l'internet, participe, en fait, à favoriser la propagation de comportements à risque dans cette sphère cybernétique. En effet ils entretiennent notamment le sentiment de puissance, l'illusion d'anonymat et l'impression d'insaisissabilité de la part des utilisateurs des terminaux numériques, dans leur communication via les réseaux et média sociaux, toute chose conjuguée qui favorise la possible prolifération de comportements déviants sur ces plateformes. Ces facteurs d'ordre philosophico - technologique concernent des aspects autres que normatifs et juridiques uniquement. Pour une pertinente réaction étatique, réparatrice, répressive ou même préventive de la propagation des déviances sur internet et les média sociaux, il importe que soient convoquées des solutions intégrant la grille d'analyse philosophico - technique de l'internet et des média sociaux, et en n'ignorant néanmoins pas les déterminantes de nature juridico-normative.

---

suivants. En effet, «*la mondialisation, ce n'est pas simplement l'amplification des échanges, c'est la mise en compétition des systèmes économiques et sociaux. Toute la question est de savoir si ce phénomène est de nature à valoriser le système non marchand (culturel) des sociétés ou si au contraire de la prise en compte des systèmes sociaux dans la compétition conduira à considère ceux-ci comme des coûts*». Z. Laidi, *Malaise dans la mondialisation*, Paris, 2001, pp. 45-47.

[17] L'auteur et à sa suite nombre de ses contemporains parle d'ailleurs à ce propos de cyberculture. Sur ces points voir W., Gibson, *Neuromancien*, Paris, Coll. J'ai lu, 1992, N° 23, p. 57: J., Huet, *Quelle culture dans le cyber-espace et quels droits Intellectuels pour cette cyber-culture*, Paris, 1998, p. 185.

B - L'ARGUMENTAIRE D'ORDRE JURIDICO-NORMATIF LIÉ À L'INTERNET

La doctrine s'accorde aujourd'hui à soutenir que l'univers de l'internet et des média sociaux a bousculé le concept d'Etat-Nation et a même généré la crise de la souveraineté de l'Etat, notamment sur le terrain de la norme, du droit et de la régulation[18]. On parle même aujourd'hui davantage de médiarchie ou, et mieux: de médiacratie pour désigner la tendance contemporaine de la gouvernance cybernétique par les médias sociaux, à côté des cadres institutionnels étatiques traditionnels, lesquels média sociaux informent et même forment les publics en imposant leurs temporalités[19]. Cette crise des institutions étatiques dans l'accomplissement de leurs missions régaliennes de gouvernance sociétale, ne manque pas d'avoir des effets sur la prolifération des comportements à risque sur les plateformes numériques.

A la réalité, la révolution cybernétique a conduit d'un coté à la multiplication des nouveaux acteurs transnationaux et des modèles institutionnels *sui generis* qui, s'ils sont souvent générés sous des auspices étatiques, ne font pas toujours l'unanimité parce que bien souvent, soit ils échappent à la seule emprise de ces Etats, soit ils en expriment trop l'empreinte à la défaveur du sentiment d'équité et d'objectivité. Ils sont de la sorte décrédibilisés dans leur participation à la régence et à l'instauration de l'ordre public dans le cyberespace[20]. Nous citerons, dans ce sens, des initiatives tels que l'*Internet Society* (I.S.O.C.)[21], *Internet Corporation for Assigned Names and Numbers* (I.C.A.N.N.)[22], et l'*Internet Engineering Task*

---

[18] M. Chawki, Essai sur la notion de cybercriminalité, I.E.H.E.I., juillet 2006, p.13.

[19] Y. Citton, Démocratie ou médiarchie ?, *I.N.A. Global*, N° 2, juin 2014, p.1. L'auteur souligne d'ailleurs que les média sociaux opèrent nécessairement comme des «médiateurs», re-constituant et re-configurant les termes et cadres sociétaux dans lesquels ils s'insèrent. Ils prennent aujourd'hui plus que jamais réellement part à la configuration de la gestion de la cité, au point de ne plus pouvoir ou devoir être ignorés.

[20] M. Chawki, *ibid*.

[21] L'*Internet Society* a été fondée en 1992. Son objectif est la promotion et la coordination d'Internet. Autorité morale et technique, elle réunit les fonds et légalise les processus de standardisation. Des grandes entreprises mondiales y participent. Elle est organisée en chapitre dans chaque pays (Cf. M. Chawki, *ibid*.). Elle a aujourd'hui 89 034 membres individuels, 87 organisations membres et 129 chapitres et groupes de l'intérêt spécial.

[22] Organisation à but non lucratif créée en 1998. Elle a remplacé l'*Internet Assigned Numbers*, fondée par Jonathan Postel. Elle gère l'unicité et la répartition des noms de domaine. Elle s'apprête à gérer le cœur technique du réseau depuis son

Force (I.E.T.F.)[23].

D'un autre côté ensuite, l'environnement virtuel de l'internet et des média sociaux pose des difficultés non négligeables quant à l'effectivité de la régulation étatique dans la perspective traditionnelle qui s'est toujours faite dans la sphère réelle. En effet, interpellant plusieurs acteurs aussi bien institutionnels que non, et convoquant de la sorte plus d'un ordre juridique, le cyberespace bouscule les problématiques liées à l'application de la loi en l'occurrence pénale, avec beaucoup de pierres d'achoppement. Ces dernières sont ainsi relatives à divers points. Il s'agit notamment du choix de la loi applicable en cas de cyber délinquance, c'est-à-dire de la détermination de la compétence susceptible de légiférer les hypothèses de comportements anti sociaux sur internet et les média sociaux. Il s'agit tout aussi du choix de la juridiction compétente pour trancher les litiges ici, entendu que les infractions cybernétiques ont le plus souvent un caractère empreint d'extranéité[24]. Aussi, face à ces difficultés et bien d'autres qui rendent complexe la saisine de ce type de délinquance par les seuls dispositifs normatifs nationaux, la coopération juridique internationale, conjuguée d'une mutualisation des approches de prévention et de répression, se présente telle comme un moyen efficace d'enrayer la prolifération des comportements à risque sur internet et les média sociaux. Si l'on peut aisément être d'accord avec cela, il reste à déterminer la configuration possible de cette coordination et de cette mutualisation pour lutter contre cette prolifération.

---

absorption de l'Authority Root Server. Elle est composée de 19 membres. Cette organisation qui bat pavillon américain a bien souvent fait l'objet d'houleux débats quant à son objectivité dans la répartition des noms de domaines et la gouvernance de l'internet à l'échelle mondiale, et dans sa concussion de par son implication dans les relations internationale à la faveur de certains Etats occidentaux. Source in M. Chawki, *ibid*.

[23] Il s'agit d'un groupement libéral et informel de bénévoles. Il est supervisé par l'*Internet Engineering Steering Group*, et par l'*Internet Architecture Board*. Il est responsable de l'évolution des standards Internets. Il est divisé en six domaines d'application: *Applications Area, Operations et Management Area, Routing Area, Security Area, Transports Area, et Users Services Area*, M. Chawki, *ibid*.

[24] S. El Zein, «L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie», *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, *op. cit*., p. 153.

II - LA CONFIGURATION POSSIBLE DE L'APPROCHE MUTUALISÉE ET COORDONNÉE DE LUTTE CONTRE LA PROPAGATION DES COMPORTEMENTS À RISQUE SUR INTERNET ET LES MÉDIA SOCIAUX

Il s'agit, à ce niveau, de s'appesantir sur les figures que peut prendre la démarche ici urgemment postulée. En transformant le monde en un village global, internet contribue à faire prendre conscience que nous sommes exposés au même risque. De la même manière que le développement des corporations avait suscité l'émergence des mutuelles d'assurance, cela devrait faire comprendre la nécessité de mutualiser et de coordonner la lutte contre la cybercriminalité. Cette nécessité admise, il reste à déterminer les schémas envisageables de cette impérative mutualisation des mécanismes de lutte contre la propagation de comportements à risque à travers internet et les média sociaux (A) et comment elle peut être coordonnée (B).

A - LES SCHÉMAS ENVISAGEABLES DE LA NÉCESSAIRE MUTUALISATION DES MÉCANISMES DE LUTTE CONTRE LA PROPAGATION DE COMPORTEMENTS À RISQUE À TRAVERS INTERNET ET LES MÉDIA SOCIAUX

Entendue comme la démarche consistant à mettre en commun des moyens de diverses natures, qu'ils soient humains, financiers, logistiques ou de toute autre nature, afin d'optimiser l'atteinte de certains résultats, la mutualisation passe pour être une des approches recommandées dans la saisine des problématiques se spécifiant par leur variété de facteurs. De la sorte, et dans le cadre de lutte contre la prolifération des comportements à risque sur internet et les média sociaux, la mutualisation envisageable ici procède par une approche multisectorielle (1), et le partage notamment des expériences à succès dans la répression de la cyber délinquance (2).

1 - L'APPROCHE MUTUALISÉE PAR UNE DYNAMIQUE MULTISECTORIELLE DE MISE EN COMMUN DE RESSOURCES DIVERSIFIÉES

A la réalité, face à des agissements dont la prospérité est, comme on l'a vu, liée à des facteurs interpellant plusieurs aspects tantôt philosophico-technologiques et tantôt juridiques ou normatifs, il est opportun que la réponse à y donner soit tout aussi multisectorielle. La prolifération des comportements à risque à travers internet et les média sociaux impliquant diverses déterminantes dans sa genèse et dans sa fortune, leur résorption impose en effet de recourir à une démarche basée sur une mise en commun de mécanismes de natures diversifiées. De façon concrète, la mutualisation postulée ici, interpelle la convocation de moyens d'ordre aussi bien technologique et juridique, que ceux liés à la formation ou à l'information des usagers des N.T.I.C., du réseau internet et des média sociaux. A titre d'illustration, on ne saurait se contenter d'élever des barrières uniquement normatives et juridiques face à ces agissements dangereux, dont les acteurs n'ont de cesse de performer les intelligences pour contourner les limites, failles et retard de la norme par rapport à l'évolution de la science et de la technologie. En effet et au-delà du punitif, il est urgent et pertinent que les restrictions d'ordre technologique et l'encadrement juridique répressif, soient conjugués à des mesures préventives et pédagogiques de formation et d'information des usagers, notamment jeune, sur les conséquences sociétales dommageables de certains agissements sur cette sphère. On pourrait prendre ici école à partir des cas d'exposition spontanée et sans réserve des évènements de leur quotidien par les internautes et autres usagers des plateformes numériques, exposition certes voulue, non malsaine à la base, mais non sans conséquence sur les atteintes futures à la vie privée, à l'intégrité morale et aux données personnelles desdits usagers.

C'est dire que la démarche urgemment postulée de mutualisation par une dynamique multisectorielle serait d'un impact certain dans la lutte contre la prolifération des comportements à risque sur internet et les média sociaux. Il n'en va pas très différemment de l'approche mutualisée par le partage des expériences technologiques ou normatives à succès.

2 - L'APPROCHE MUTUALISÉE PAR LA MISE EN COMMUN DES EXPÉRIENCES TECHNOLOGIQUES OU NORMATIVES À SUCCÈS

Autant il est opportun de convoquer diverses solutions de façon multisectorielle, autant il est indiqué de s'inspirer des expériences ayant été couronnées de succès dans certains Etats et systèmes juridiques pour venir à bout d'une déviance n'épargnant aucun point sur la planète. Ce versant de la mutualisation des expériences procède, en effet, de la transposition, dans la mesure du possible, dans un Etat donné, des modèles à succès avéré dans d'autres Etats. Afin de lutter contre la propagation des comportements à risque sur internet et les média sociaux, une approche ainsi mutualisée, pourrait dans ce sens impliquer une configuration pouvant prendre une double forme.

La première qu'on pourra nommer la mutualisation des expériences normatives et judiciaires, s'assimile à l'inspiration du droit comparé ou de la jurisprudence. Elle est relative au partage des solutions juridiques mises en œuvre dans le cadre de réactions étatiques *ante* ou *post delictum* à la prolifération des états dangereux dans la sphère virtuelle. Dans ce cadre et pour adapter le contexte normatif ou judiciaire des pays technologiquement moins avancés à l'évolution technologique qui s'impose, on pourrait ainsi prendre exemple sur des cas où des mesures de sûreté préventives ou des véritables sanctions originales, ont été édictées avec succès dans des pays technologiquement évolués. Par ailleurs, une harmonisation des législations pourrait faciliter la lutte dans la mesure où il y aurait plus de correspondance entre les incriminations d'un pays à l'autre. Ce qui, du coup, pourrait faciliter non seulement la répression des infractions même commises à l'étranger, mais aussi l'extradition des auteurs. De même, il pourrait être intéressant de s'inspirer de procédés judiciaires réussis de lutte contre la cybercriminalité dans d'autres ordres juridiques.

La seconde forme que pourrait prendre la mutualisation des expériences ici, serait le partage des solutions technologiques au sens d'obstacles ou de restrictions de nature technique tels que conçus et développés sous d'autres cieux pour résorber la prolifération des agissements cyber délinquants. L'universalité de la technologie de l'internet et des médias sociaux aujourd'hui postule en effet à soutenir qu'une solution technologique développée dans un

pays donné pour lutter contre la prolifération des comportements cybercriminels, peut assurément être transposé dans un autre pays faisant face aux mêmes préoccupations. Cette mutualisation des expériences technologiques passe nécessairement, il faut en convenir, par la due considération des droits de la propriété intellectuelle et assimilés sur les solutions technologiques réalisées dans d'autres espaces en matière de cybercriminalité.

Par cette double configuration, l'impérative mutualisation des mécanismes de lutte contre la propagation des comportements à risque sur internet et les réseaux sociaux, serait assurément atteinte. Il convient de s'attarder également sur la figure que peut prendre la nécessaire coordination de ces mécanismes.

B - LA COORDINATION CONCEVABLE DES MÉCANISMES DE LUTTE CONTRE LA PROPAGATION DES COMPORTEMENTS À RISQUE SUR INTERNET ET LES MÉDIAS SOCIAUX

Par essence, la coordination s'entend d'une collaboration concertée. Elle désigne, d'après le *Vocabulaire juridique* du Doyen Cornu, un ordonnancement destiné à mettre en liaison et en ordre des éléments complémentaires, un effort d'harmonisation entre eux[25]. La coordination permet d'assurer la cohérence des politiques normatives aussi bien que des procédures en vue d'atteindre des objectifs communs. On doit y comprendre un ensemble de démarches, qui, tenant compte de la diversité des systèmes juridiques et des difficultés qui en résultent, tendent à en atténuer les effets pervers[26]. La coordination convoque l'harmonisation des textes juridiques de prévention ou de répression des agissements déviants ici visés, tout autant que la coopération judiciaire pour résorber leur prolifération sur les plateformes numériques. L'approche coordonnée implique de la sorte une configuration qui peut s'exprimer sur un double plan: le premier tient à la substance des normes et consiste en l'harmonisation des textes ici concernés (1), et le second la coopération judiciaire en cette matière (2).

[25] G., Cornu, *Vocabulaire juridique*, 11ème édition, Association Henri Capitant, Paris, P.U.F., Quadrige, 2016, p.1057, voir *coordination*.

[26] Sur tous ces développements cf. G., Cornu, *ibid*

1 - L'HARMONISATION NÉCESSAIRE DES TEXTES VISANT LA LUTTE CONTRE LES COMPORTEMENTS À RISQUES SUR INTERNET ET LES MÉDIAS SOCIAUX

Le premier axe de la coordination qui peut sinon doit impérativement être envisagé consiste, en effet, en l'urgente harmonisation des textes implémentant la lutte contre la prolifération des comportements à risque sur internet et les réseaux sociaux. Cette harmonisation textuelle peut ainsi se concevoir sur le terrain de l'incrimination de ces agissements, *i.e.* «*le fait pour le législateur de rendre un comportement criminel*»[27].

Il s'agit de l'érection d'un agissement en infraction en précisant les déterminantes de sa constitution et de sa sanction[28]. Dans ce sens, l'incrimination procède non seulement de l'identification de l'interdit pénal dont s'agit par la précision de ses éléments constitutifs, mais aussi de la définition de la sanction qui doit y être suivie et, par extension, l'encadrement juridique de sa répression au sens de déterminantes juridiques de la responsabilité pénale de son auteur. En matière de cybercriminalité, le caractère manifestement international des paradigmes qui gouvernent la commission des actes criminels, impose une démarche harmonisée entre les différents ordres juridiques nationaux en présence, aussi bien dans l'identification juridique des interdits pénaux que dans la définition de leurs suites pénales, c'est-à-dire dans le cadre de leur incrimination.

En effet, une mise en harmonie de la définition des interdits pénaux permet d'abord d'universaliser les catégories et biens juridiques protégés. L'un des écueils en matière de cybercriminalité consiste souvent, en fait, en la disparité des interdits pénaux selon les ordres juridiques en présence. A titre illustratif, un comportement peut être incriminé dans un Etat et être permis dans un autre. Cette antinomie pourrait poser problème au cas où sa commission se fait dans la sphère virtuelle de l'internet en mettant aux prises les lois nationales des deux Etats. Cette dissonance normative ne manque pas d'avoir une influence sur la cohérence des mécanismes de lutte

[27] Pradel J., *Droit pénal général*, *op.cit*., p.235: Manacorda S., «La théorie générale de l'infraction pénale en France: lacunes ou spécificités de la science pénale ?», *R.D.P.C*., 1999, pp.35 – 53, cité par F. Nguele Mballa, La protection pénale du patrimoine immatérielle en droit camerounais: le cas des biens de la propriété intellectuelle, *op. cit*, p.119.
[28] P., Rossi, *Traité de droit pénal*, 3ème édition, *Paris*, 1863, p.248.

contre la prolifération des comportements à risque à travers internet et les média sociaux. Il y a donc urgence d'une harmonisation des dispositifs normatifs affectant la définition des interdits pénaux cette matière.

En outre, cette urgence d'une coordination normative des incriminations s'exprime tout aussi s'agissant de l'harmonisation des réponses pénales aux comportements à risque sur les plateformes numériques. L'harmonisation ici procède en fait d'une mise en cohérence des réponses pénales permettant ainsi une lutte pertinente contre la propagation des comportements ici incriminés dans un contexte où la commission des actes cybercriminels interpelle plus d'un ordre juridique national. A titre illustratif, la définition d'une sanction pénale peu sévère comme devant accompagner la commission d'un acte cybercriminel dans un Etat à la différence d'un autre, peut générer une disparité répressive qui ne va pas sans incidence sur la fragilité des mécanismes de lutte contre la propagation des comportements criminels.

2 - LA COOPÉRATION JUDICIAIRE REQUISE DANS L'OPÉRATIONNALISATION DE LA RÉPRESSION DES COMPORTEMENTS À RISQUE SUR INTERNET ET LES MÉDIAS SOCIAUX.

Le second plan, davantage, institutionnel et procédural concerne tout aussi l'impératif de coordination des actions à entreprendre, mais qui tient cette fois d'un aspect principalement formel pour lutter contre la prolifération des comportements à risque sur internet et les média sociaux. Entendu comme un univers de communication et de partage informationnel, constitué d'infrastructures, de réseaux et de systèmes d'information ou de communications électroniques, mondialement interconnectés[29], le cyberespace, qui accueille internet et les média sociaux, est à la réalité un espace immatériel dénué de frontières de toutes sortes. Ceci nourrit les débats autour de l'opportune coopération des Etats, par exemple dans la recherche de la preuve numérique ou l'attraction des responsables des actes délinquants devant des juridictions. En effet et en pratique, l'identification

[29] B. , Spitz (Sous la présidence de), Le droit pénal à l'épreuve des cyberattaques, *Rapport du groupe de travail français sur la cybercriminalité*, Paris, Mars 2021, p.11.

des auteurs de ces infractions s'avère complexe en raison de la dimension internationale de la cybercriminalité et donc des difficultés inhérentes à l'obtention de la preuve et d'indices numériques, la plupart du temps situés à l'étranger. Il faut dire à la réalité qu'infortunément, les Etats brandissent très souvent à propos, l'étendard de leur souveraineté, compliquant ainsi les réponses à entreprendre pour lutter contre la propagation des comportements à risque sur internet et les média sociaux. C'est dire qu'une approche interpellant la coopération et l'harmonisation des procédures de prévention ou de répression de ces déviances permettrait de lutter contre leur prolifération est plus qu'urgente. D'une manière générale, il importe de procéder par une coordination des entreprises dans ce sens. Nous flirtons ici véritablement avec des questions liées à la problématique de l'absence de frontières normatives dans la médiacratie et la régulation de l'internet, lesquelles questions ne manquent pas d'actualité ni d'intérêt en droit international privé s'agissant de l'immatériel en général et de la répression de la cybercriminalité en particulier.

Il est, en effet, impératif de recourir à une coopération judiciaire répressive dans le cadre des procédures permettant de rechercher les preuves numériques, de définir la loi applicable et la juridiction compétente, et d'attraire les cybers délinquants devant les dites juridictions dans le cadre de procédés assimilables à l'extradition pénale. Des expériences ont certes déjà été entamées dans ce sens, mais il importe qu'elles soient amplement poursuivies.

Au total, organiser la lutte contre la propagation de comportements à risque à travers internet et les média sociaux, c'est tenir compte de l'ensemble des différents paradoxes qu'impose le numérique, notamment la très célère évolution des N.T.I.C. par rapport à la norme sensée y être appliquée, laquelle célérité conjuguée à divers autres facteurs impose, comme on l'a vu, une urgente mutualisation et coordination des mécanismes et politiques normatives à propos. Du point de vue pénal notamment, cet impératif de mutualisation et de coordination procède de la nécessaire adaptation des réponses pénales aux spécificités des interdits pénaux constitutifs de la cybercriminalité et à la conjoncture technologique de notre temps. En la matière, les exemples qui existent déjà peuvent être utiles[30].

[30] On peut signaler à cet effet tous les mécanismes de coopération judiciaire et policière qui existent déjà en Afrique centrale et tous les efforts déployés dans le cadre de la lutte contre cette autre criminalité internationale que constitue le blanchiment des capitaux et le financement du terrorisme.

LES ENJEUX ECONOMIQUES DU CYBERESPACE

Désiré AVOM
Agrégé des Facultés de Sciences Économiques
Doyen de la Faculté des Sciences Economiques et de Gestion, Université de Yaoundé II, Soa

INTRODUCTION

L'espace est considéré depuis les années 1940 avec l'article séminal de Lôsch (1940) non seulement comme un substrat à l'économie mais davantage comme un adjuvant. L'espace n'est pas le lieu, mais il est plus large que celui-ci. Pour Aristote, repris par Morand (1966), l'espace est la somme de toutes les places occupées par le corps. Il est considéré non pas comme le vide mais comme un tout donc l'usage est multiforme. Perroux en 1950, à la suite de la distinction faite par les classiques, considère trois données pour caractériser l'appartenance à l'espace. Pour l'auteur, l'appartenance d'homogénéité ou la similitude constitue la première donnée. Ensuite nous avons l'appartenance de polarisation ou dépendance et enfin l'appartenance de planification ou l'organisation. Quelle que soit sa considération, l'espace est devenu un bien économique, un champ d'analyse de plusieurs disciplines au confluent de l'économie.

L'espace ne présente plus un obstacle dont la distance entre les pays renforcerait de faibles interdépendances. Avec les prouesses de la technologie, accélérées par la diffusion de l'internet, l'espace est un facteur d'accélération de la production nationale (Claval, 2008: Demoustier et Itçaina, 2022). Cette dimension de facilitateur de la production a donné lieu

à un champ d'analyse en économie à savoir l'économie spatiale qui connait de nos jours deux variantes principales: l'ancienne économie spatiale et la nouvelle économie spatiale. Si l'ancienne économie spatiale intègre les analyses fondées sur le local et le global dans un sens de régionalisation encore connu sous le nom d'économie régionale, la nouvelle économie spatiale se veut plus large. Elle rassemble, en effet, l'économie régionale et l'économie internationale avec un fort ancrage des nouvelles technologies de l'information et de la communication (Gaudard, 2004).

C'est en fondant ses analyses sur la nouvelle économie spatiale qu'est décrit le concept de cyberespace[1] qui fleurit d'éloges et de récriminations de nos jours tant les enjeux sont divers et variés. On doit à William Gibson dans sa nouvelle *Gravé sur Chrome*, publiée en juillet 1982, la première occurrence du terme cyberespace qui désigne alors une représentation graphique de données extraites des mémoires de tous les ordinateurs du système planétaire. Pour Levy (1990), le cyberespace désigne l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle. Il désigne moins les nouveaux supports de l'information que les modes originaux de création, de navigation dans la connaissance et de relation sociale qu'ils permettent. Davantage popularisé par le renforcement de la mondialisation au début des années 1990, le cyberespace est de nos jours considéré comme un risque énorme pour les pays en développement car très vulnérables aux attaques cybernétiques, mais plutôt comme une source de richesses pour les pays développés puisqu'il est utilisé pour renforcer la concurrence sur les marchés et anticiper sur le futur des relations économiques entre les pays.

Quelques faits montrent l'ampleur du cyberespace dont on ne saurait dissocier de la montée fulgurante de l'interconnectivité mondiale. D'après la Banque mondiale (2022), en janvier 2021, le monde comptait 7,83 milliards d'habitants une progression de 80 millions de personnes chaque

[1] Le cyberespace est défini comme «l'informatique en réseau», selon la formule proposée par le *Livre blanc* de 2008. En effet, apparemment, le cyberespace est perçu comme un espace sans frontières, qui se joue non seulement des cadres physiques mais aussi juridiques. Dès lors, l'opinion courante affirme aisément qu'il n'y a pas de frontières dans le cyberespace et que celui-ci conduit à leur effacement (Kempf 2015).

année. En janvier 2021, on estimait à 4,66 milliards le nombre de personnes connectées dans le monde, soit 316 millions (7,3 %) de plus comparé à la même période en 2020: 5,22 milliards de personnes utilisent le mobile sur la terre soit 66,6 % de la population mondiale totale (e-works, 2022). Le nombre d'utilisateurs des réseaux sociaux ne cesse d'augmenter. Aujourd'hui ils sont 4,20 milliards à surfer sur les médias sociaux dans le monde, soit 490 millions de plus en un an, ce qui équivaut à plus de 53 % de la population mondiale totale. En 2021, un habitant possédant un smartphone passait en moyenne 4 heures et 10 minutes sur son appareil. Parmi les utilisateurs de smartphone, 90,7 % surfent sur des applications de messagerie**:** 88,4 % utilisent des apps de médias sociaux, 69,4 % font des achats en ligne, 67,2 % de vidéos et jeux de divertissement, 61,8 % de maps, 52,9 % de musique, 52,9 % de jeux gaming, 38,7 % de services financiers, 29,4 % de santé et de fitness et enfin 11,4 % de rencontre.

La forte dépendance à internet ces dernières années s'est renforcée par la sédentarité causée par la pandémie à coronavirus. Le nombre de cyberattaques a explosé et se regroupe de nos jours au tour de 10 catégories: Attaque par déni de service et par déni de service distribué; attaque de l'homme au milieu; hameçonnage et harponnage; téléchargement furtif; cassage de mot de passe; injection; cross-site Scripting; écoute clandestine; attaque des anniversaires et logiciel malveillant. Cette multiplicité d'attaques témoigne à suffisance la portée d'un contrôle de l'activité cybernétique qui n'est pas seulement malveillante mais au contraire, le cyberespace concourt au développement économique des pays.

Cette brève analyse cherche alors à répondre à la question suivante: quels sont les enjeux économiques du cyberespace ? Pour y apporter quelques éléments de réponses, nous segmentons notre analyse en six points. Après la présentation de quelques clés de compréhension du cyberespace (1) , nous apprécions le cyberespace, tour à tour, comme un renforcement de la géographie économique (2), un adjuvant de la mondialisation (3), une source d'externalités, d'incitations et d'opportunités (4) un réducteur d'asymétries d'information (5) et une source de dépenses importantes (6).

I - LE CYBERESPACE: QUELQUES CLÉS DE COMPRÉHENSION

HISTORIQUE

La première occurrence du terme cyberespace remonte à la contribution séminale de William Gibson en 1982, en tant que représentation abstraite des relations entre les systèmes de données. Apparu aux États-Unis pendant la guerre froide, le cyberespace s'est largement développé et étendu au monde entier depuis les années 1990, au point qu'il devenu difficile d'en établir les frontières, au regard de la distances qui lie des individus résidents dans les deux extrémités du globe mais qui communique et échange des informations en temps réel. Plus tard, en 1996, John Perry Barlow, fondateur de l'EFF (*Electronic Frontière Fondation,* ONG internationale de protection des libertés) et considéré comme l'un des pionniers d'Internet, écrit la *Déclaration d'indépendance du cyberespace*. Contrairement à la cybergéopolitique qui implique l'avènement des nouvelles technologies, en tant que moteur du capitalisme actuel dont l'émergence remonte à la troisième révolution industrielle (1970-2000) avec Jérémy Rifkin, le cyberespace trouve son essor dans la quatrième révolution industrielle (2010 à aujourd'hui). Depuis la création du *World Wide Web* par Tim Berners-Lee en 1991 (aussi appelé «la toile»), l'économie mondiale n'a fait que se numériser, suite au changement sociétal profond, et est connectée en temps réel avec l'arrivée de l'Internet mobile grâce à la création des smartphones. Le cyberespace est un réseau de communications constitué d'éléments physiques et immatériels, résultant de l'interconnexion des individus, des entreprises ou des États (appelés internautes) à travers des outils tels que les ordinateurs, les téléphones mobiles ou les tablettes numériques. Ainsi, le cyberespace rend possible la circulation d'informations à travers le monde à grande vitesse tout en favorisant de multiples pratiques de collaborations transnationales, telles que le cofinancement (crowdfunding), la coproduction de savoirs (wiki), la cohabitation et même le covoiturage. Cet espace, à la fois virtuel et réel,

pose cependant quelques questionnements sur sa délimitation, la domination de certains acteurs et la nécessité de sauvegarder la souveraineté des États à travers le monde.

ACTEURS

Les acteurs du cyberespace sont multiples et variés. L'on distingue des acteurs dits classiques à savoir les États, les firmes transnationales, les acteurs non étatiques, les organisations de cyberdéfense institutionnalisées. C'est le cas par exemple des États Unis avec les GAFAM (Google, Amazone, Facebook, Apple, Microsft), la Chine avec l'essor des BATX (Baidu, Alibaba, Tencent, Xiaomi). Toutefois, le cyberespace a favorisé l'émergence de nouveaux acteurs tels que les pirates informatiques, les **organisations hacktivistes (**Anonymous, WikiLeaks…), les groupes criminels et/ou les terroristes agissant pour des motifs politiques, ou des cybercriminels motivés par le profit, ou même des sociétés militaires/de sécurité privée.

ENJEUX

Le cyberespace constitue un enjeu de rivalités de pouvoir entre les acteurs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques. Le cyberspace, comme de nombreux territoires ou régions de notre planète, représente des enjeux importants dans le contexte des tensions géopolitiques actuelles. Les États essayent d'imposer leurs lois et politiques, tout en souhaitant contrôler l'immense quantité de données échangées sur la toile. En conséquence, les armes sont remplacées par les technologies sophistiquées et par les systèmes de sécurité de plus en plus puissants afin de se prémunir des cyberattaques et des menaces sur la sécurité des donnés. Ces aspects cristallisent de nouvelles menaces liées à la cybercriminalité ou l'utilisation des réseaux informatiques dans le cadre de conflits politiques, de combats militaires, de guerre économique, de renseignements ou de politique d'influence diplomatique et culturelle. Le développement du cyberespace participe clairement à l'établissement d'une cyberdiplomatie, à travers la formation des alliances numériques. C'est le

cas par exemple de la fameuse alliance *Five Eyes* qui regroupe les grandes puissances numériques mondiales, à l'instar des États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada. Par ailleurs, le cyberespace est un enjeu de conflictualité traduit par l'hameçonnage (extorquassions des coordonnées bancaires des personnes), l'espionnage (introduction dans un système pour y dérober des données), le sabotage (empêcher le fonctionnement efficient du système), les subversions (actions visant à affaiblir les pouvoir d'une organisation jusqu'à son effondrement).

CARACTÉRISTIQUES

Le cyberespace agrège la sphère de l'Internet, la sphère des technologies mobiles, la sphère de la géolocalisation, et la sphère du nouvel Internet des objets. Outre l'intangibilité relative, l'opacité, la mutabilité, la pervasivité, la mobiquité, la dualité, la complexité et la résilience, sans prétende à l'exhaustivité, l'on associe également au cyberespace les caractéristiques suivantes:

- L'universalité: le cyberespace constitue la surface du globe, et est présent dans tous les aspects de nos vies;
- L'inattribution: le cyberespace est celui de la transparence absolue, de l'accès immédiat à toutes les données. Cet anonymat de la belligérance est stratégiquement nouveau;
- La non-létalité: les actions les plus conflictuelles ne sont pas létales (aujourd'hui du moins);
- La fragilité: l'existence de points singuliers de vulnérabilité et le potentiel de défaillances en cascade (effet domino);
- L'absence de diversification: la parcellisation du futur Internet autour d'écosystèmes numériques contrôlés par quelques géants.

LE CYBERESPACE: UNE DÉMATÉRIALISATION DES FRONTIÈRES PHYSIQUES

Le cyberespace ne répond pas nécessairement à la norme de

délimitation physique des frontières étatiques. Il englobe un ensemble d'utilisation et d'intervenants de tous les pays, reliés et interconnectés par des moyens virtuels. Ainsi, il constitue une perte de souveraineté des états à travers ses flux transfrontaliers dont une partie échappe au contrôle des autorités nationales (Kempf, 2015). Cette dématérialisation a donné naissance à de nouveaux défis tels que la cybercriminalité et la facilitation des flux financiers illicites vers les paradis fiscaux. Ce phénomène a été accentué par le la mondialisation, corollaire de la dérèglementation des flux des biens et des personnes à travers le monde. D'après les analyses de Boulanger (2014), ces nouveaux enjeux ont donné naissance à d'autres domaines tels que la cyber-offensive, la cyber-défense ou le cyber-espionnage dont les acteurs sont aussi bien les Etats que les entreprises et les individus. Ainsi, des pans entiers de la connaissance et de l'activité humaine sont désormais transformés en données numériques dont le volume connaît une croissance exponentielle (Douzet, 2020).

LE CYBERESPACE: UNE DÉPENDANCE FACE AUX GÉANTS DU WEB

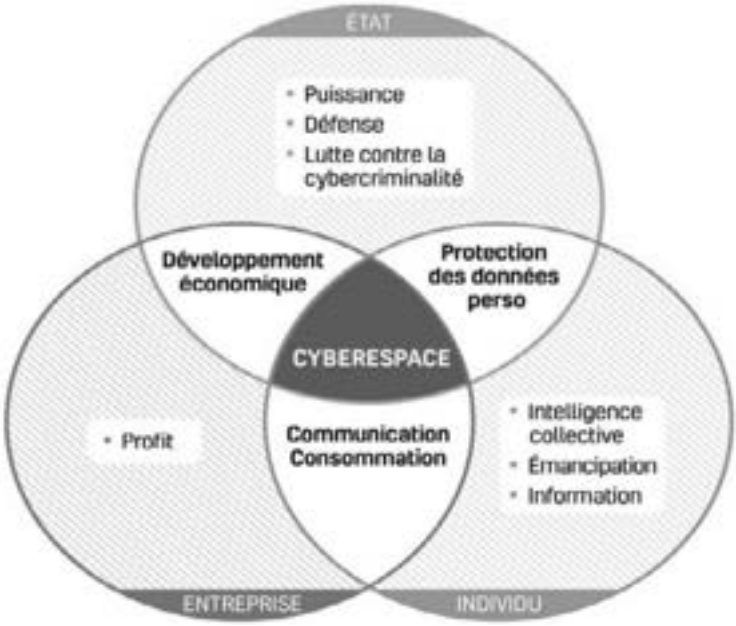
L'utopie originelle du cyberespace, défendue notamment par Barlow (1996) dans *la Déclaration d'indépendance du cyberespace,* soutient l'absence de régulation d'Internet et de gouvernance. Le cyberespace ne se situe pas dans les frontières des États. Cet idéal d'indépendance du cyberespace vis-à-vis des États est valorisé par les grandes entreprises du Web: parce que leurs activités se déploient dans le cyberespace, ces entreprises échappent en grande partie à l'impôt. Or, bien que les services proposés par ces entreprises soient le plus souvent gratuits, les profits tirés de l'utilisation des données personnelles sont considérables.

LE CYBERESPACE: UNE MENACE DE LA SOUVERAINETÉ ?

De plus en plus, le cyberespace avec ses dérives et ses enjeux soulève avec acuité la question de la souveraineté des États. En effet, il n'échappe pas totalement aux frontières des États qui cherchent à réguler son

fonctionnement de différentes manières: interdiction de certaines pratiques, mise en place d'une fiscalité adaptée, lutte contre la cybercriminalité, etc. Ainsi, la capacité d'un États à défendre son cyberespace face aux nombreuses cyber-attaques qui menacent les systèmes d'information est devenu un enjeu majeur de sécurité et de puissance. Au Cameroun par exemple, la cyberactivité est régulée par l'Agence de Régulation des Télécommunications, suivant la loi N°2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité. En Chine, le cyberespace fonctionne comme un réseau national limité par des frontières, parfois qualifiées de «grande muraille numérique». Ce réseau est relié au cyberespace mondial mais les échanges sont contrôlés. La censure, opérée par des milliers d'agents qui observent l'activité des internautes, y est très présente. Les spécificités du cyberespace nécessitent de repenser la souveraineté étatique telle qu'elle s'exerce traditionnellement sur un territoire.

LE CYBERESPACE ET LA COALITION TRIPARTITE



2 - LE CYBERESPACE COMME UN RENFORCEMENT DE LA GÉOGRAPHIE ÉCONOMIQUE

L'explosion des communications *via* les différents réseaux qui constituent le cyberespace et dont internet, est un véritable défi pour la géographie économique. En effet, définie comme l'étude de la répartition spatiale et la localisation des activités économiques, la géographie économique se spécialise sur les questions de localisation industrielle et l'accès aux services de télécommunication et de transport notamment (Thomas, 2004). L'enjeu du cyberespace pour la géographie économique, à cet effet, peut être observé sur ces dimensions.

Au niveau industriel, le cyberespace permet la constitution d'une Base Industrielle et Technologique du Numérique (BITN) capable de produire des matériels et des logiciels sur des segments tels que la technologie quantique, l'analyse des données de masse, le blockchain et l'intelligence artificielle (Gasançon, 2018). L'un des premiers apports de l'intelligence artificielle en ce domaine consiste à conseiller la Direction des Systèmes d'Information (DSI) sur le choix des territoires d'implantation des différents matériels (serveurs des sites internet de l'entreprise par exemple) afin de disposer du régime législatif le plus favorable (Kempf et Mazzucchi, 2015). De la même manière, le choix des partenaires pour les matériels, les logiciels ou, plus encore, les *clouds* de l'entreprise, doit être mûrement réfléchi et analysé. A titre d'exemple, la grande proximité entre acteurs industriels et étatiques dans certains pays (Chine, Russie, mais aussi États-Unis) peut ouvrir la porte à des tentatives d'espionnage industriel à visée souveraine. Dans ce cadre, le cyberespace, par la connaissance des partenaires potentiels et de leurs réseaux d'affiliation, peut permettre d'éviter des brèches fondamentales dans la sécurité de l'entreprise. En outre, il permet également le regroupement des entreprises de différentes tailles allant des Start up innovantes, jusqu'aux entreprises de taille internationale. Il permet en outre le développement des offres sur les marchés concurrentiels internationaux (Dhas et Vetrivel, 2020).

Sur le plan des services de télécommunication, le cyberespace permet

l'accès à des applications sur de multiples plates-formes et des services du e-commerce (El Manir, 2019). Ces services incluent notamment l'échange électronique entre entreprises et gouvernement (B2G), le commerce en ligne d'entreprise à entreprise (B2B), l'échange électronique entre une entreprise et ses employés (B2E), le commerce en ligne à destination des particuliers (B2C), et le commerce en ligne entre particuliers (C2C). Enfin, à travers le cyberespace de nombreuses entreprises proposent des services sur Internet, payants ou non, tels que les banques, assurances, presses, radios et TV/films en ligne.

S'agissant des services de transport, le cyberespace permet la fluidité logistique et d'aménagement des territoires (Guilleux, 2018). Par le canal des Technologies de l'Information et de la Communication (TIC), il permet la modernisation des transports maritimes avec les signaux émis par les navires qui permettent de retracer les routes maritimes, ce qui est aussi un instrument des politiques de sécurité maritime. C'est également un moyen de facilitation des échanges dans les communautés portuaires et les mobilités urbaines (David et Saidi-Kabèche, 2006). Par-delà, il constitue un moyen de développement des corridors, qui sont des outils majeurs de l'économie de la circulation (Georgopoulou, 2014). Grace au numérique, les corridors, tout comme les villes qu'ils relient entre elles, sont désormais connectés grâce aux réseaux des opérateurs de téléphonie mobile.

Le cyberespace, au-delà de ses enjeux, est surtout un espace stratégique de la circulation des informations en temps quasi-réel. En ce sens, internet constitue une mondialisation puisque presque aucun lieu sur la planète n'est maintenant isolé des autres (Kempf et Mazzucchi, 2015). L'on peut ainsi savoir de manière immédiate ce qu'il se passe de l'autre côté du globe, ce qui permet de réagir au plus vite aux évolutions politiques, économiques ou sécuritaires.

Ces enjeux géographiques diffèrent, toutefois, selon ses acteurs, notamment les Firmes Transnationales (FTN) et les Etats[2]. Pour les FTN, le cyberespace est synonyme croissance économiques considérables et

[2] https://www.kartable.fr/ressources/geopolitique/cours/le-cyberespace-conflictualite-et-cooperation-entre-les-acteurs/56585 .

stratégies de localisation. Le cas par exemple des cinq grandes firmes américaines qui dominent le marché du numérique mondial, Google, Apple, Facebook, Amazon et Microsoft (GAFAM) dont la croissance a été exponentielle durant les récentes décennies. Ce sont des entreprises qui ont été créées dans les années 1990-2005 et dont les chiffres d'affaires ont été multipliés par 5 entre 2009 et 2018. Cette croissance s'explique par des mécanismes économiques tels que l'«*effet réseau*»: l'utilité croît avec le nombre d'utilisateurs. Ensuite, les économies d'échelle: produire en grande quantité permet de réduire les coûts. Enfin, l'efficacité de la stratégie: les FTN font appel à la séduction de l'intelligence, de l'affect et du désir de l'individu et jouent sur l'illusion de la gratuité. A titre d'exemple, on considère que 97 % des revenus de Facebook sont issus de la publicité.

Pour les États, le cyberespace représente un défi stratégique et constitue une composante importante de leur puissance. Ils peuvent être espionnés sur Internet ou subir des cyberattaques. Ce qui rend primordial la sécurisation des installations contre les cyberattaques et le contrôle des informations qui circulent (désinformation, théories du complot, etc.).

3 - LE CYBERESPACE COMME UN ADJUVANT DE LA MONDIALISATION

Le cyberespace est décrit également comme formé de trois couches: la couche matérielle avec les ordinateurs, les serveurs, les banques de données et les infrastructures physiques qui permettent les échanges (Kempf 2015: Lespinois 2017). La couche logicielle qui regroupe les programmes qui font tourner les échanges à travers des protocoles et des processus techniques: la couche sémantique qui donne du sens à l'information en permettant d'associer des chaînes de caractères, en permettant grâce à de puissants algorithmes de créer de l'information en regroupant, en croissant ou en géolocalisant des données. Son périmètre est assez difficile à cerner précisément car le cyberespace est le milieu où circulent les données numériques (Lespinois 2017).

Le cyberespace, grâce à l'émergence des nouvelles technologies de l'information et de la communication, a connu une croissance sans

précédent au cours des dernières décennies: ceci a affecté différentes dimensions de la vie de l'homme, incluant la sphère politique, économique, social et culturel. Les effets du cyberespace sont majorés par notre dépendance aux technologies de l'Internet et par l'interdépendance globale de toutes les infrastructures informatiques mises en réseau: y compris avec les infrastructures vitales au fonctionnement de notre société. Ces biens matériels sont soumis aux contraintes de la géographie physique et politique. Ces infrastructures étant dépourvues de sécurité intégrée, les données non chiffrées qui circulent via les câbles sont faciles à aspirer.

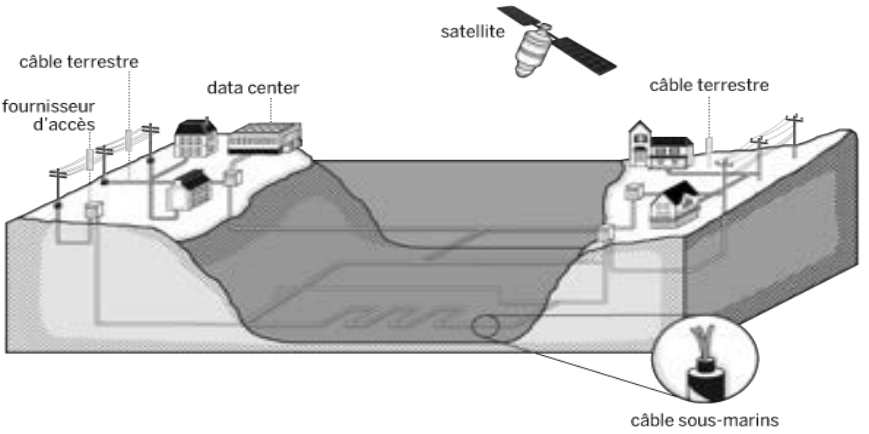


Figure 1: Circulation des données à travers les trois couches du cyberespace
Source: Données compilées par Su, Salamatian, Grumbach du laboratoire LISTIC (Université de Savoie), de l'Académie des Sciences de Chine et de Datasphere-Inria

La principale caractéristique du cyberespace réside dans son extension mondiale. Après l'air, l'espace extra-atmosphérique, le cyberespace constitue le milieu le plus englobant. Le réseau internet exploite cette caractéristique du cyberespace pour étendre sa toile à la surface de la terre. La nature globale de la galaxie internet a été rendue possible par le fait qu'elle est gérée par un seul organisme, *l'Internet Corporation for Assigned Names and Numbers* (ICANN), qui attribue les noms de domaine.

Le cyberespace est central dans la dématérialisation des échanges financiers, dans l'augmentation des échanges d'informations, mais aussi dans celles très rapides des échanges de biens, de services et entre les

hommes. En effet, grâce au cyberespace, les flux financiers n'ont jamais été aussi productifs et fluides: la nanoseconde devient l'unité de temps de déclenchement des ordres de Bourse. Les écrans sont les seuls témoins des transactions et les fortunes ne se matérialisent plus dans des livres de comptes, mais bien dans les seuls serveurs informatiques. Il devient nettement moins risqué, et certainement plus rentable au regard de la peine encourue, d'opter pour un détournement de fonds *via* une cyberattaque que de persister à vouloir s'en prendre physiquement aux coffres d'une agence bancaire (Arpagian 2016). Le cyberespace façonne l'expérience des internautes et leur permette de communiquer, d'échanger et d'innover. Des recherches aux boutiques en ligne en passant par la messagerie et les voyages et plus encore, les acteurs à ce niveau de l'économie numérique rivalisent pour le regard, l'attention et le portefeuille des internautes. De nos jours, ce marché est dominé par un petit nombre d'entreprises, qui offrent certains des services les plus populaires d'Internet. Plusieurs de ces entreprises jouent un rôle de plateforme ou de marché multidimensionnel, ce qui signifie qu'elles offrent une base sur laquelle d'autres applications, processus ou technologies peuvent être développés.

Les cinq plus grosses sociétés au niveau des applications de nos jours sont Alphabet (la société mère de Google), Amazon, Tencent, Facebook et Alibaba:

- On estime que Facebook et Google reçoivent 84 % des investissements mondiaux (hors Chine) en publicité numérique[3].
- On estime que 49,1 % des dépenses de consommation en ligne aux États-Unis en 2018 ont été faites sur Amazon. De manière similaire, on estime que près de 60 % du marché du commerce électronique en Chine est détenu par Alibaba.
- Google à lui seul représente 90 % du marché mondial de la recherche sur internet[6], plus de 60 % des navigateurs web, (de loin) le premier système d'exploitation mobile (Android)[1], la plus importante plateforme de vidéos générés par les utilisateurs

[3] Investopedia (2018). *Les 10 plus grandes sociétés Internet mondiales*. Disponible à l'adresse: https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp

(Youtube), en plus de compter plus de 1,5 milliards d'utilisateurs de son service de messagerie (Gmail).

- Facebook, qui inclut Facebook Messenger, WhatsApp et Instagram, domine les médias sociaux et la messagerie à l'échelle mondiale et détient 4 des 6 plus importantes plateformes de médias sociaux au monde.

Tencent est propriétaire de WeChat, la plus importante plateforme de médias sociaux en Chine, qui compte plus d'un milliard d'utilisateurs actifs mensuels. L'éventail de plateformes de Tencent, qui inclut QQ, WeChat et divers produits de médias sociaux et de contenus sous la marque Tencent, capte presque 4 fois plus l'attention des utilisateurs qu'Alibaba et Baidu combinés. (Investopedia 2018). La figure 2 présente l'utilisation des différents services internet américains et chinois en Chine. Il ressort de cette figure que, bien que la Chine soit l'un des leaders mondiaux, cependant, même dans son pays les services américains restent les plus utilisés.

Ces multinationales technologiques construisent des environnements numériques composés de plateformes multiples dans divers espaces, ce qui leur vaut d'être appelées des conglomérats ou géants numériques. Leur présence se fait surtout sentir au niveau des applications d'Internet, mais elles offrent, de plus en plus, de services et d'infrastructures en nuage, comme nous le verrons par la suite. Elles ne sont pas seulement les plus grandes sociétés Internet: elles comptent également parmi les plus importantes au monde.

Les plateformes numériques sont généralement des marchés bilatéraux, en ce sens qu'elles développent des espaces ou plateformes utiles. D'une part, les gens obtiennent les produits et services qu'ils souhaitent, et d'autre part, les entreprises peuvent trouver des clients. Ces plateformes obtiennent des parts de marché dans leurs marchés respectifs par le biais de leur contrôle des données et d'effets de réseau (lorsque la valeur du service pour l'utilisateur augmente parallèlement au nombre des autres utilisateurs).

4 - LE CYBERESPACE COMME SOURCES D'EXTERNALITÉS, D'INCITATIONS ET D'OPPORTUNITÉS

En plus d'être un espace d'échange d'idées, le cyberespace procure des opportunités économiques et industrielles, qui dans un monde connecté et 'globalisé' favorisent le développement économique.

Le cyberespace en général est d'une grande importance dans un contexte où les marchés physiques sont de plus en plus saturés, par exemple en ouvrant de nouvelles opportunités commerciales, notamment dans les pays émergents. Il y aurait donc des avantages partagés selon la Banque mondiale à ce que les pays entrent dans le cyberespace et participent au 'libre marché'. D'une part, cela favoriserait le développement économique et social. D'autre part, les puissances économiques pourraient profiter de ces nouveaux marchés pour se maintenir et continuer leur expansion (Deichmann et al, 2016). Dans un contexte de forte compétition à l'échelle mondiale où seuls le savoir-faire industriel et financier et la capacité d'innover font la différence, le cyberespace offre donc l'opportunité aux Etats et aux entreprises de briser les barrières et de connecter à l'espace d'un temps différents marchés situés à des zones et pays différents. Les marchés financiers par exemple sont désormais interconnectés et un volume important d'informations et d'échanges s'opèrent entre les pays, ce qui concourt à générer plus de richesse. Ainsi, à partir du développement technologique et du numérique, de nombreuses entreprises de divers secteurs d'activités, incluant les banques, les établissements de santé, les assurances, les fournisseurs des services de communication... font usage massivement du cyberespace pour booster leur compétitivité et améliorer leur productivité. Cependant, les opportunités que confère le cyberespace sont généralement sources de multiples incitations entre les pays, ce qui *in fine* produits des externalités généralement négatives. L'information étant la clé du succès des économies et du fonctionnement des cyberespaces, les pays sont généralement incités à manipuler et contrôler l'information pour préserver un avantage économique sur leurs concurrents. Selon El Manir (2019), l'enjeu des pays dans le cyberespace reste le contrôle de l'information, et ce, sous différentes facettes et à des fins de propagandes

pour par exemple freiner le développement ou la commercialisation des produits dont les concurrents ont un certain avantage, pour acquérir de nouvelles connaissances et pour sauvegarder ses propres données.

En conséquence, les externalités de ces cyber-nuisances et cyber-attaques vont conduire à ce qui est communément appelée «cybercriminalité», c'est-à-dire l'ensemble des crimes et délits traditionnels ou nouveaux réalisés via les réseaux informatiques.

En termes de cyber-nuisance, l'Afrique remporte la palme de la cybercriminalité. Cette situation ne cesse d'être dénoncée. 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.

Selon le Rapport PWC (2021), de manière globale, le secteur financier, les télécommunications et les services publics sont les cibles par excellence de la cybercriminalité. Ainsi, les récentes attaques cybercriminelles ont été portées sur le secteur financier. L'exemple le plus connu est la cyber-attaque dont a été victime l'Estonie en 2007, interrompant et paralysant toutes les transactions de ses banques. De même en 2016, la Banque centrale du Bangladesh, a été victime d'un piratage informatique, et a perdu 81 millions de dollars. Une banque équatorienne est attaquée la même année et a enregistré des pertes d'environ 10,7 millions d'euros.

En ce qui concerne l'Afrique, d'abord l'affaire rapportée par la presse mondiale faisant état que des dispositifs chinois ont été mis en place lors de la construction du siège de l'Union Africaine, ce qui leur a permis de

transférer chaque nuit, l'intégralité du contenu des serveurs du bâtiment de l'organisation africaine vers des ordinateurs situés à Shanghai. Ensuite sur le plan financier, 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). Pour l'année 2016, elle a la Cote d'ivoire a estimé un préjudice lié à la cybercriminalité d'environ 1,8 milliard FCFA (plus de 2,5 millions EUR) dans le pays, causé en grande partie par la multiplication des fraudes aux moyens de paiement électroniques et par l'augmentation des infractions entre pays africains (Rapports DITT, 2016). La figure ci-dessous reporte quelques chiffres clé des activités de cybercriminalité en Afrique ces dernières années.

Figure 3: Quelques chiffres clés sur la cybercriminalité en Afrique

Source: Rapport PWC (2021)

Source: Rapport PWC (2021)

5 - LE CYBERESPACE COMME RÉDUCTEUR D'ASYMÉTRIE D'INFORMATION

L'asymétrie est une notion qui s'emploie en biologie, en logique, mais aussi en économie, en stratégie militaire. En économie, l'asymétrie de l'information est associée à la question du fonctionnement des marchés et de la concurrence dite «parfaite», le concept décrit la situation où des agents

disposent d'informations pertinentes que d'autres n'ont pas[4](Akerlof, 1970). L'asymétrie d'information peut être destructrice de la rationalité des agents économiques. En stratégie militaire, le conflit asymétrique est un conflit où «les adversaires n'ont ni le même statut, ni les mêmes critères de victoire ou de défaite, ni les mêmes règles et méthodes, ni n'emploient les mêmes moyens…Terrorismes, guérillas, désordres mafieux conflits dans les zones de non-droit…, sont des conflits asymétriques» (Chartron et Broudoux, 2015).

La notion de cyberespace traduit un univers dont la gouvernance, la régulation, les alliances, sont devenus des enjeux majeurs dans un contexte d'économie globalisée mais aussi de déploiement opaque d'une cybercriminalité devenue centrale, mettant en cause la sécurité des États. L'affaire Snowden a publiquement mise en lumière ce dessous des cartes (Pétiniaud, 2014). La guerre électronique est engagée et les États y consacrent plus que jamais une part importante de leur budget. Que ce soit le piratage massif de *Sony Pictures*[5] ou les attaques en déni de service, la lutte contre le cybercrime s'organise aujourd'hui avec ses conférences et de nouveaux diplômes dans des écoles spécialisées en cybersécurité.

Le cyberespace se caractérise, avant tout, par l'ensemble des réseaux informatiques, électromagnétiques, connectés entre eux à diverses fins, qu'elles soient militaires, économiques ou civiles. Il s'agit, en quelque sorte, d'un réseau des réseaux, permettant à une multitude d'acteurs de communiquer, d'échanger et faire transiter de l'information. Qu'il s'agisse des activités boursières: informations militaires (en partie seulement): ou encore de structurer les communications des forces de l'ordre, tous utilisent les mêmes protocoles de communication entre serveurs, ainsi que les mêmes câbles de fibre optique que n'importe quelle vidéo YouTube ou page Facebook. Il est donc fondamental de retenir que tout dans le cyberespace est interrelié et qu'une attaque contre une partie de cet espace peut avoir de grandes répercutions sur les autres activités (Chartron et Broudoux, 2015).

[4] Voir les travaux du professeur Joseph E. Stiglitz a reçu en 2001 le prix Nobel d'économie, avec George A. Akerlof et A. Michael Spence pour «leurs travaux sur les marchés avec asymétrie d'information»

[5] http://abonnes.lemonde.fr/pixels/article/2015/01/28/piratage-de-sony-la-france-doute-de-la-piste-nord-

Bien avant l'apparition du cyberespace, une des ressources les plus importantes pour la conduite de la guerre a toujours été l'information. Afin de viser les bonnes cibles ou de faire les bonnes manœuvres militaires, il était déjà nécessaire de posséder de 1'information. La pénétration des technologies du cyberespace dans nos sociétés a créé un nouveau type de dépendance à l'information, l'élevant au rang de valeur la plus importante des sociétés modernes (Choucri et Goldsmith, 2012). Dans cet espace, tout devient d'une façon ou d'une autre, une bribe d'information dématérialisée, convertie en signaux électriques ou lumineux, acheminée d'un système à l'autre.

LA CYBERGUERRE ET ASYMÉTRIE D'INFORMATION

Dans *Cyber war*: *The next threat to national security and what to do aboutit*, Clarke et Knake définissent la cyberguerre comme étant des «actions by a nation-state to penetrate another nation' s computers network for the purposes of causing damage or disruption» (Clarke et Knake 2010). Cette définition centrée sur les États doit être comprise au sens large: un acte de cyberguerre est la mise en œuvre de cyberattaques visant à perturber les réseaux informatiques d'un autre État dans le but de causer des dommages ou de rendre non opérationnels ces réseaux. Le déclenchement de la cyberguerre n'est toutefois pas simplement une affaire de puissances étatiques: des acteurs non étatiques comme des individus, des groupes politiques ou encore des entreprises privées pourraient être à la source de cyberguerres.

La cyberguerre est donc une forme de conflit et d'affrontement dont les enjeux sont généralement liés aux systèmes d'information et de renseignement, dans un contexte d'interconnexion des réseaux et des infrastructures. Dans ce type de guerre, «la barrière à l'entrée ne se jauge pas tant en volumes de budgets ou d'effectifs militaires, mais davantage en termes d'imagination» (Arpagian, 2009). Cela favorise donc de nombreux acteurs non étatiques ou n'étant pas nécessairement en position de force dans le système international. Les pays émergents pourraient ainsi utiliser la facilité d'accès au cyberespace et leur imposante population formée afin

de mener des cyberattaques massives, voire des actes de cyberguerre.

La cyberguerre se trouverait donc à la croisée des chemins: elle se situe dans un nouvel espace qui vise avant tout les réseaux technologiques et d'informations. En ce sens, elle serait donc bien une guerre pour l'information: pour son contrôle, sa diffusion et son éventuelle manipulation.

STRATÉGIES DE CYBERDÉFENSE RÉDUCTEUR D'ASYMÉTRIE D'INFORMATION

La porosité du cyberespace et la facilité avec laquelle il est possible d'y projeter de la force ont poussé certains acteurs à vouloir se doter de stratégies de cyberdéfense. Ces stratégies visent notamment la protection des réseaux étatiques, militaires et civils dans le cyberespace. Il s'agit de limiter les vulnérabilités et de se prémunir contre la perturbation des activités se tenant dans cet espace. Les stratégies de cyberdéfense les plus faciles à observer et à analyser sont celles mises en avant par les États, puisqu'elles sont majoritairement publiques. D'autres acteurs comme les entreprises privées ou les organisations internationales ont également mis en œuvre des cyberstratégies. Ces dernières sont toutefois plus difficiles à évaluer, car elles ne sont généralement pas publiques et que ces acteurs ne publient que rarement de l'information sur les attaques dont ils ont été victimes.

Certains pays ont par exemple basé leur développement dans le cyberespace aussi bien dans la défense que dans l'attaque. Cette situation implique que malgré toutes les capacités d'attaque, les États-Unis et les autres pays développés sont vulnérables comparés à des pays moins développés ou mieux protégés. Cette vulnérabilité a d'importantes répercussions sur toutes les autres sphères d'action. Il s'agit d'un élément clé de l'utilisation par des acteurs non-dominants de technologies dans le cyberespace puisque la vulnérabilité peut devenir le talon d'Achille de pays développés, les dissuadant d'intervenir dans des conflits locaux ou régionaux, de peur d'être victimes de cyberattaques massives. D'une façon paradoxale, la technologie censée amélioré le fonctionnement de la société

devient en quelque sorte la condition propice à la conduite de guerres asymétriques pouvant être dévastatrices pour les acteurs dominants (Clarke et Knake 2010).

LA GOUVERNANCE DANS LE CYBERESPACE RÉDUCTEUR DE L'ASYMÉTRIE D'INFORMATION

En ce début de siècle, la domination américaine provoque encore un ensemble de contestations et d'alliances afin de renverser le contrôle des États-Unis. Notamment le groupe de puissances constitué du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud (BRICS) est perçu comme un ensemble contestataire particulièrement important dans les questions liées à la gouvernance du cyberespace. Ces pays se sont démarqués par leur approche revendicatrice et contestataire de la gouvernance du cyberespace. Deux courants principaux sont présents dans la contestation du modèle actuel: l'un souverainiste qui vise la prise en charge locale des questions reliées à l'Internet, mais coordonnée par une organisation intergouvernementale: alors que le second s'appuie sur des organisations internationales visant à encadrer vraiment le cyberespace et à limiter la puissance américaine.

Au cœur des BRICS, il est possible de voir ces deux courants à l'œuvre. L'Inde, le Brésil et l'Afrique du Sud (IBSA) cherchent, par exemple à développer un ensemble de stratégies et de protocoles de coopération en plus d'alliances politiques (Ebert et Maurer 2014). La Russie et la Chine sont, quant à eux, considérés comme plus opportunistes, jouant à la fois sur les terrains de la collaboration avec d'autres puissances émergentes tout en essayant de faire des gains individuels. Il existe donc de grandes différences d'opinions sur les modèles de gouvernance à adopter dans le cyberespace.

Certains pays comme le Brésil et l'Afrique du Sud ont favorisé l'inclusion de la société civile dans la gouvernance de l'Internet alors que la Chine a maintenu un contrôle strict par1 'État et que la Russie a tendance à emprunter une stratégie alliant contrôle et inclusion partielle de tierces parties. Entre ces groupes de pays, il existe également une tension entre contrôle étatique et liberté économique des marchés dans la gestion et la

mise en place de l'Internet. Ces différences rendent plus difficile l'adoption d'une vision commune de ce que devraient être Internet et sa gouvernance (Ebert et Maurer 2014, 283). Le type de régime joue donc un rôle important dans le type de positions concernant la gouvernance du cyberespace (Ebert et Maurer 2014, 287).

Ces distinctions dans les modèles de gouvernance mis en avant par les différents pays des BRICS créent un double dynamique: il existe une volonté de créer un véritable équilibre des forces face aux États-Unis, mais aussi face à certaines puissances montantes. De façon paradoxale, afin d'atteindre cet équilibre au sein des puissances montantes, certains pays comme l'Inde ou le Brésil ont décidé de signer des accords ou des conventions avec les États-Unis.

La question de la cyberguerre est également devenue fondamentale dans le cadre actuel des relations internationales. Les enjeux de développement et d'influence qui y sont liés sont tels qu'ils ne peuvent être négligés ni mitigés. L'absence de gouvernance globale et de régime juridique fiable pour qualifier les actes de cyberguerre sont, à notre avis, deux données fondamentales pour le développement de ces conflits (Kerschischnig 2012). Il pourrait d'ailleurs s'agir d'une opportunité pour les pays émergents de devenir des «sujets» à part entière du système international, et même de renverser partiellement ou complètement l'ordre du système international. En nous basant sur des cas d'étude, nous tenterons d'identifier, dans la partie suivante, quelles sont les options pour ces pays.

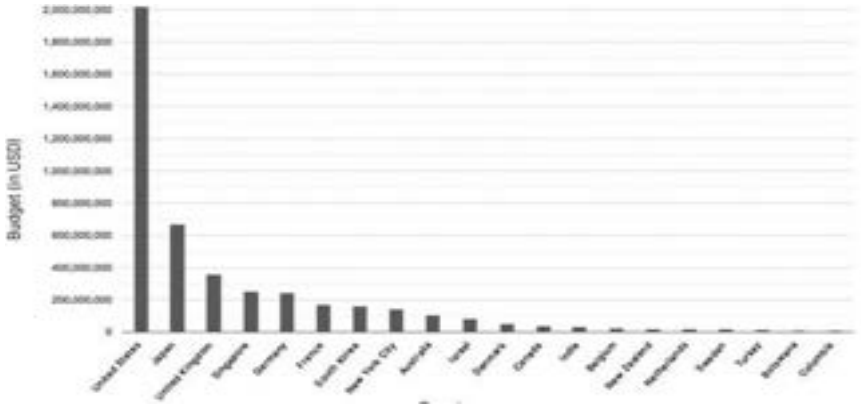
6 - LE CYBERESPACE COMME UNE SOURCE DE DÉPENSES IMPORTANTES

L'un des enjeux politique et économique les plus importants du cyberespace est celui de la défense à travers la cybersécurité (Gilad et al, 2021). C'est ainsi qu'on observe qu'à travers le monde une augmentation des dépenses de cyber-intervention, mais les dépenses varient encore considérablement. Selon une analyse récente de l'agence internationale The Record, les pays du monde entier ne semblent pas s'accorder sur le montant qu'il convient de consacrer à la cyberdéfense. Mais ces dernières années,

presque tous les pays ont augmenté leurs dépenses pour le cyberespace, particulièrement la cybersécurité.

A l'échelle mondiale, bien qu'il soit difficile de comparer les investissements en matière de cybersécurité d'une région à l'autre les budgets sont rarement rendus publics. Grâce à des entretiens avec des fonctionnaires, des demandes de documents publics et des estimations d'organismes universitaires et gouvernementaux, l'agence internationale The Record a pu obtenir un aperçu de l'énorme écart de dépenses entre les programmes de cybersécurité. Les budgets allaient de quelques millions de dollars (Colombie, Botswana) à plus de 2 milliards de dollars (États-Unis) (voir Figure 4). Par exemple, la Nouvelle-Zélande dont la population dépasse les 5 millions d'habitants, a dépensé environ 16 millions de dollars pour mettre en place son équipe d'intervention en cas d'urgence informatique. Singapour, autre pays d'Asie-Pacifique, dépense environ 250 millions de dollars par an. Selon des documents gouvernementaux consultés par The Record, le Canada, dont la population représente environ un quarantième de celle de l'Inde, alloue environ 36,7 millions de dollars par an à son Centre de cybersécurité. Cependant, la plus grande divergence dans les données se situe entre les États-Unis et les autres pays. L'Agence de cybersécurité et de sécurité des infrastructures du pays, dispose d'un budget de plus de 2 milliards de dollars, ce qui représente pratiquement le triple de celui du Japon (665 millions de dollars). Il éclipse également les budgets du Royaume-Uni (350 millions de dollars, selon des documents publics), de l'Allemagne (240 millions de dollars) et de l'Agence nationale de cybersécurité de la France (165 millions de dollars).

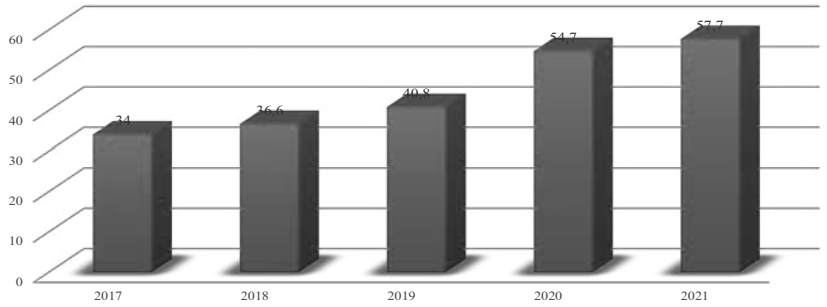
Figure 4: Comparaison des dépenses de cybersécurité (en milliards de dollars US) en 2017



Source: The Record

Nous observons également à travers la figure 5 l'évolution des dépenses de cybersécurité dans le monde durant la période 2017-2021. Nous constatons que les dépenses de cybersécurité sont passées d'environ 34 à 57,7 milliards de dollars US: soit une augmentation de 23,7 milliards. Compte tenu de l'importance du cyberespace et particulièrement de la cybersécurité pour le développement économique, plusieurs experts indiquent les dépenses dans ce domaine ne vont cesser de croitre comme cela été observé malgré la pandémie de COVID-19.

Figure 5: Dépenses de cybersécurité dans le monde de 2017 à 2021 (en milliards de dollars américains)



Source: Statista 2021[6]

[6] https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/#statisticContainer.

Malgré les avancées indéniables du développement du cyberespace en Afrique, cette partie du monde reste marquée par une vulnérabilité persistante. 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 (El Manir, 2019). En termes de cyber-nuisance, l'Afrique remporte la palme de la cybercriminalité. Cette cybercriminalité africaine à un coût. 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). Une étude de *l'International Data Group Connect* estime que chaque année, les cybercrimes coûtent à l'économie sud-africaine 573 millions de dollars. Au total, le continent a enregistré une perte de 3,5 milliards de dollars pour l'année 2017 (El Manir, 2019).

Le gouvernement camerounais a intensifié ses efforts pour la lutte contre la cybercriminalité. En effet, cybercriminalité fait des ravages dans tous les pays du monde. Le gouvernement camerounais a dépensé 14 milliards de francs CFA entre 2016 et 2017 pour sécuriser le cyberespace du pays. Il s'agit d'une enveloppe qui provient du Fonds Spécial des Télécommunications (FST) du ministère camerounais des Postes et Télécommunications, alimenté par les contributions des entreprises de télécommunications opérant au Cameroun et rendu accessible à l'Agence Nationale des TIC. Selon des sources officielles, l'Agence Nationale des TIC (ANTIC) a reçu cette enveloppe pour financer la mise en œuvre d'activités et l'acquisition de divers équipements dans le cadre d'un programme de sécurisation de l'internet au Cameroun. En raison de l'évolution rapide de la technologie, le pays est devenu de plus en plus vulnérable à la cybercriminalité, ce qui a entraîné d'énormes pertes financières pour les particuliers, les organisations et même le gouvernement camerounais.

Selon l'ANTIC, toute une série d'opérations de cybercriminalité sont

actuellement répandues au Cameroun. Le *«skimming»* (fraude à la carte bancaire), le *«scamming»* (fraude financière en ligne), le *«Web defacement»* (modification non autorisée de la page d'accueil d'un site web), ou le *«spoofing»* (usurpation d'identité), la fraude à la *Simbox* qui est un boîtier électronique permettant de se faire facturer le trafic téléphonique international au tarif national, entre autres ont déjà été répertoriés par l'agence[7].

Compte tenu des dégâts causés par la cybercriminalité, le dévouement de l'ANTIC est compréhensible. Le *scamming* a coûté au Cameroun environ 4 milliards de francs CFA ces dernières années, selon l'agence. Le *skimming* a également coûté à l'État camerounais environ 3,7 milliards de francs CFA. Le piratage des installations de télécommunications, ainsi que des infrastructures sensibles comme les aéroports, les gares et les métros, est également fréquent. Le cyber-terrorisme est une préoccupation majeure.

CONCLUSION

Faisant suite au développement des nouvelles technologies et d'internet, la cybercriminalité, concerne l'ensemble des infractions commises via un système informatique généralement connecté à un réseau. Elle pose de défis juridique, géopolitique, technique et culturel énormes aux États et aux organisations. La lutte contre la cybercriminalité est une composante essentielle d'une politique de défense et de sécurité des systèmes d'information. Eu égard les conventions internationales de portée générale, les menaces spécifiques à la cybercriminalité restent perceptibles et induisent l'impérieuse nécessité de poursuivre des objectifs défensifs et non offensifs. De plus, face aux menaces terroristes, l'offensive contre la cybercriminalité s'avère légitime du fait de son organisation complexe autour de réseaux contre lesquels il est difficile de lutter. Toutefois, l'atténuation des risques cyber dans un contexte de COVID 19, nécessite une généralisation du télétravail, un renforcement des aspects liés au capital humain, aux processus et à la technologie y compris la conformité.

[7] Près de 8 milliards perdus à cause du *«scamming»* et du *«skimming»*.

La résurgence de la cybercriminalité contraint les Etats à l'adoption des mesures visant à disposer d'une résilience et d'une capacité d'intervention pour faciliter les échanges d'informations techniques et opérationnelles utiles. Il importe par ailleurs, de consolider la gouvernance numérique pour la cybersécurité et la cybercriminalité afin d'assurer une gestion effective des risques et cyber menaces. De mettre en place un programme de cyber résilience visant à minimiser les dommages subis suite à un cyber attaque.

RÉFÉRENCES BIBLIOGRAPHIQUES

1 Akerlof, G. A. (1970). The Market for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84, 488-500.

2 Arpagian, N. (2009). La cyberguerre: la guerre numérique a commencé. Paris: Vuibert.

3 Arpagian, N. (2016). L'Europe de la sécurité numérique: très juridique, mais guère technologique, et encore insuffisamment économique. In *Annales des Mines-Réalités Industrielles,* 3, 51-54.

4 Banque Mondiale (2022). Données statistiques.

5 Chartron, G., Broudoux, E. (2015). Enjeux géopolitiques des données, asymétries déterminantes. Document numérique et société, May 2015, Rabat, Maroc.pp.67-83.

6 Choucri, N. D., Goldsmith, (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, 68(2), 70-77.

7 Clarke, R. A., Knake, R. K. (2010). Cyber war: the next threat to national security and what to do about it. 1st edition. New York: Ecco.

8 Claval, P. , Les espaces de l'économie. *Annales de géographie*, 2008, 664, 3-22.

9 David, A., Saïdi-Kabèche, D. (2006). L'impact des TIC: logistique, transport, relation de service, organisation. La Documentation française.

10 Deichmann, U., Goyal, A., Mishra, D. (2016). Will digital technologies transform agriculture in developing countries? *Agricultural Economics*, 47, 21-33.

11 Demoustier, D. et Itçaina, X. (2022). Ancrages et polarisations territoriales de l'économie sociale et solidaire: Le PTCE Sud Aquitaine en perspective comparée. *Revue d'Économie Régionale & Urbaine*, 43-65. https://doi.org/10.3917/reru.221.0043

12 Dhas, D. B., Vetrivel, S. C. (2020). Cyberspace has greatly helped entrepreneurs to flourish. *Journal of Critical Reviews*, *7*(7), 149-152.

13 E-works (2022). https://www.e-works.fr/blog/chiffres-internet-france-monde-2021/ consulté le 27 mars 2022.

14 Ebert, H., Tim, M. (2014). Revendications sur le cyberespace et puissances émergentes. *Hérodote*, 152-153 (1), 276-295.

15 El Manir, M. (2019). Le Cyberespace Africain: un Champ aux Contradictions Manifestes/Africa's Cyberspace: A Field of Clear Contradictions.

16 El Manir, M. (2019). L'Afrique face aux défis protéiformes du cyberespace. Policy Paper, Policy Center for the New South, December 2019.
17 Gasançon, C. (2018). Le cyberespace, nouvel espace de souveraineté à conquérir», Centre des hautes études militaires (CHEM). Renseignement, Criminologie, Crises, Cybermenaces (ESDR3C).
18 Georgopoulou, C., Kakalis, N. M., Psaraftis, H. N., Recagno, V., Fozza, S., Zacharioudakis, P., Eiband, A. (2014). Green technologies and Smart ICT for sustainable freight transport. In *Efficiency and Innovation in Logistics* (pp. 15-33). Springer, Cham.
19 Gilad, A., Pecht, E., Tishler, A. (2021). Intelligence, cyberspace, and national security. *Defence and Peace Economics*, *32*(1), 18-45.
20 Gaudard, G. (2004). La nouvelle économie spatiale. *Revue d'Économie Régionale & Urbaine*, 453-463. https://doi.org/10.3917/reru.043.0453
21 Guilleux, C. (2018). Technologies de l'information et de la communication dans les transports et les échanges ouest-africains. Appel à contribution. Calanda, https://calenda.org/440169
22 Kempf, O., Mazzucchi, N. (2015). Cyberespace et intelligence économique. *Geoeconomie*, (5), 45-58.
23 Kempf, O. (2015). Cyberespace et dynamique des frontières. *Inflexions*, (3), 141-149.
24 Kerschischnig, G. (2012). Cyberthreats and international law. The Hague: Eleven International Publishing.
25 Lespinois, J. (2017). La territorialisation du cyberespace: la fin de la mondialisation? *Prospective et stratégie*, (1), 47-56.
26 Levy P. (1990), *Les Technologies de l'intelligence*. Paris: La Découverte.
27 Lôsch A., (1940). Die raumliche Ordnung der Winschafi,Yêna. The Economics of Locarion, Yale
28 Morand P., 1966, L'analyse spatiale en science économique, Paris.
29 Perroux F., I 950, L'espace économique, Paris.
30 Petiniaud L. (2014). Cartographie de l'affaire Snowden. *Hérodote*, 152-153(1), 35-42.
31 Rapport DITT (2016). Rapports d'activité de la Police Nationale de Côte d'Ivoire, pour les années 2015 et 2016.
32 Rapport PWC (2021). Les enjeux et défis de la cybersécurité en Afrique francophone subsaharienne. Résultats de l'enquête de Mars 2021.
33 Thomas, I. (2004), Géographie économique. Encyclopædia Universalis: https://www.universalis.fr/encyclopedie/geographie-economique/.

PANEL 4: QUEL AVENIR SÉCURITAIRE, QUELLE COMMUNICATION ET QUEL DÉVELOPPEMENT À L'ÈRE DES MENACES LIÉES À LA MÉDIACRATIE CYBERNÉTIQUE?

MEDIAS INTERNATIONAUX EN LIGNE ET INSECURITE: PERSPECTIVE D'UNE NOUVELLE GOUVERNANCE A LA LUMIERE D'UNE APPROCHE CRITIQUE DE LA SECURITE AU CAMEROUN

Guy Mvelle
Professeur de relations internationales
Secrétaire général de l'Université de Dschang-CMR
Coordonnateur du Master Cybersécurité gouvernance sécuritaire

INTRODUCTION

C'est toujours honnête d'adresser des félicitations à ces corps d'Etat, qui de par leurs délicates missions, sont obligés d'être relativement fermés au public, mais qui pourtant invitent et prennent en charge les universitaires pour venir discuter des questions par définition sensibles comme la sécurité dans son acception la plus large. Dans un domaine où l'information circule en circuit fermé, et où les réformes peuvent prendre suffisamment du temps pour être implémentées, inviter des personnes qui par définition ont la parole libre, pour apporter un regard critique sur les questions à traiter, est une preuve d'ouverture et d'acceptation de la controverse, seul ferment où peut aisément germer la prospérité et la paix. Je remercie à cet effet le ministre délégué à la présidence en charge des forces armées, et à travers lui, le Général de Brigade/ Directeur Général de l'EIFORCES, et toutes l'équipe d'organisation pour m'avoir associé à la discussion autour d'un sujet aussi important que celui de la médiacratie en lien avec le développement du numérique. C'est avec les universitaires qu'on comprend le monde qui nous entoure, et c'est à partir de leurs réflexions

théoriques que de nouvelles recettes sont élaborées pour répondre aux enjeux pressants de la modernité.

La conviction qui anime les organisateurs de ce colloque est que les médias en ligne sont vecteurs d'insécurité et par conséquent contribuent à freiner le développement au sein des pays qui en ont besoin comme le Cameroun. Le développement de ces médias s'accompagnerait de la libéralisation des modes d'expression publique, des doctrines, opinions, allégeances contradictoires si ce n'est antagonistes, allant jusqu'au prolongement des théâtres de conflit de l'espace réel dans celui du virtuel où le contrôle de l'Etat ne serait que faiblement garanti. La guerre semble alors avoir trouvé de nouveaux espaces de déploiement des forces, de nouveaux enjeux, de nouveaux moyens et de nouveaux acteurs. Il serait alors important de questionner la corrélation éventuelle entre la propagation des nouvelles formes de menaces et l'avènement de l'ère digitale. Autrement, dit il y aurait une intimité entre la libéralisation poussée du cyberespace et la sécurité des Etats avec au rôle principal de déstabilisation des sociétés pacifiques les médias cybernétiques. D'où la nécessité de répertorier, voire de ficher les médias sociaux digitaux les plus perméables aux usages faits par des entrepreneurs directs ou indirects d'insécurité d'une part, et d'identifier ces entrepreneurs d'insécurité les plus représentés, ainsi que les modes opératoires privilégiés par les groupes jugés à risque dans leur déploiement au niveau des médias cybernétiques d'autre part. Toute chose qui laisse alors croire que les «barbares» sont parmi nous et font paniquer ceux-là qui sont chargés d'assurer la sécurité des citoyens.

Nous sommes dans ce qu'un auteur camerounais décline comme étant le débat entre le droit de savoir du public et la nécessité du secret de la part des gouvernements qui existerait dans tous les pays du monde. A chaque fois les gouvernants cherchent à contrôler l'information prétextant qu'une certaine discrétion est nécessaire pour assurer le succès de leurs charges. D'où le recours à la notion de sécurité nationale qui malheureusement n'est pas souvent bien définie[1]. Toute la littérature réaliste des relations internationales ne tourne-t-elle pas également autour de cette notion clé de sécurité qui est à son tour au cœur de l'intérêt national des Etats ? Depuis le XVIIeme siècle, Thomas Hobbes a mis dans nos esprits, l'idée pessimiste tirée de sa vie personnelle selon laquelle l'homme est par nature violent, un animal sauvage, possessif, agressif, prédateur, ignorant, par conséquent, toute organisation sociale et même tout sentiment de

[1] F., Beng Nyamnjoh: «Contrôle de l'information au Cameroun: implication pour les recherche en communication», *Afrika Spectrum*, 28, 1993, p: 93.

sociabilité. C'est le souci de préservation de soi qui le pousse à l'état de nature de laisser libre cours à ses actions qui ne peuvent être entravées à cause d'une absence d'institutions politiques susceptibles de les contraindre. Cette situation égalitaire entraîne le rapport conflictuel entre les hommes (fondements anthropologiques de l'inimitié entre les individus). En dehors de la perspective hobbesienne, les organisateurs de ce colloque sont également dans une perspective wébérienne qui offre à l'Etat le monopole de la violence légitime, et la soumission des acteurs non-étatiques comme les médias à la puissance publique. La production du discours sur la sécurité est dans ce cas un acte exclusif de pouvoir non reconnu à des acteurs dépourvus des prérogatives de puissance publique.

Pareil réquisitoire à l'endroit des médias cybernétiques mérite alors une attention particulière tant il ressemble à l'ouverture d'une croisade contre tous les porteurs des contenus éditoriaux diffusés en ligne d'une part, et tous ceux qui n'appartiennent pas à l'architecture étatique de la sécurité. Nous sommes dans une conception réaliste et néo-réaliste de la sécurité, laquelle ne l'envisage que sous la perspective étatique, et le contrat social liant l'autorité publique avec le citoyen à l'intérieur de l'Etat étant le seul cadre dans lequel peut se réaliser une coordination efficace de l'action collective. La sécurité des citoyens relèverait alors exclusivement des institutions étatiques et tous ceux qui n'y appartiennent pas, mais tiennent un discours sécuritaire, à l'instar des médias en ligne, sont considérés comme source de menace. Mais comme on le verra dans le cadre ce travail, cette conception stato-centrée de la sécurité est à réviser.

D'abord modeste, très dépendante des médias qui la développaient et largement ignorée du grand public, cette presse s'est progressivement développée à partir de la seconde moitié des années 1990 aux Etats-Unis, un peu plus tard en Europe et en Afrique. Occupant désormais la place de quatrième média d'information grand public, elle peut être définie comme le fruit du traitement journalistique de l'information avec l'usage des technologies numériques en ligne.

Dans l'examen de la médiacratie qu'entendent faire les organisateurs de ce colloque, il est important de faire avec Francis Balle une distinction entre les médias traditionnels sur le web[2], le web comme médias à part entière[3], et le web comme moyen de téléchargement[4].

---

[2] Les journaux américains furent les premiers à ouvrir un site internet dans les années 1990: Newsweek, Time, Wall Streets Journal, et en 1994 naît le premier magazine consacré à Internet: Wired.

[3] Ici il s'agit des journaux en ligne à part entière.

[4] F. Balle: *Médias et société*, 12e édition, Paris, Montchrestien, 2005, pp: 182 et s.

Au Cameroun, en dehors des médias classiques disposant de sites de diffusion d'informations en ligne, l'on ne dénombre pas moins d'une cinquantaine de titres cybernétiques pour la plupart généralistes, mais qui mettent effectivement un point d'honneur sur le traitement des différentes crises et conflits. Les plus connus sont cameroun-info.net, 237actu.com, actucameroun.com, camerounweb.com, camerounvoice.com, politudenews.com, camer.be, cameroun24.net, journalducameroun.com, cameroun-muntunews.com, etc. Si leur manière de traiter l'information liée aux crises et conflits revêt une importance heuristique certaine, c'est plutôt le cas de quelques grands médias internationaux en ligne (MIELs) qui retiendra notre attention dans le cadre de cette recherche.

De nombreux exemples incriminant les médias suite à la diffusion de contenus portant atteinte aux valeurs essentielles ou à la sécurité, notamment aux règles de sécurité opérationnelle, existent, et attestent de la perception qui est retenue d'eux dans de nombreux Etats. D'autres informations touchent à l'incitation à la violence et au moral des troupes concernent par exemple les images de cadavres, la destruction de l'arsenal de l'armée régulière ou les tortures, etc. Parfois des manipulations grossières sont détectées. Lors de la première guerre du golfe en 1991, un reporter de guerre, Marcel Trillat, est filmé en plan serré face à la caméra dans un studio à Paris prétextant qu'il est entrain de couvrir la guerre à partir de l'Arabie Saoudite tandis que défilent derrière lui des images d'archives prises par l'armée américaine en Irak lors de la bataille de Khafji, première bataille terrestre qui débute en fin janvier 1991. La raison de la manipulation est que les journalistes ne peuvent s'approcher de la zone des combats à cause des menaces des forces de l'ordre saoudiennes. En 1992, un rapport de l'ONU dénonce le rôle négatif des médias dans l'ex-Yougoslavie relevant qu'ils donnaient des informations mensongères et incendiaires et attisaient le climat de haine et les préjugés mutuels qui alimentaient le conflit en Bosnie. Au Rwanda, le génocide qui se déroule en 1994 révèle également le rôle joué par la Radio-télévision des Mille Collines qui a mené une campagne systématique d'incitation à la haine raciale et à la mobilisation des deux communautés l'une contre l'autre.

Le Cameroun connaît également une diffusion des messages d'exacerbation de l'insécurité dans le NOSO ou dans la guerre contre la secte islamique Boko Haram dans l'Extrême-nord. En 2018, une vidéo fait le tour des réseaux sociaux montrant des exactions imputées à l'armée dans la région de l'Extrême-nord. Les images montrent des hommes armés tirant sur une dizaine de personnes agenouillées face à un mur près des maisons en flammes. Cette vidéo intervient

après une première très violente diffusée sur internet mettant en scène de présumés soldats camerounais abattant deux femmes et leurs jeunes enfants. Au lendemain de la diffusion de la première vidéo, le journal Jeune Afrique titre «Cameroun: sept militaires arrêtés après la diffusion d'une vidéo sur les exactions de l'armée». D'autres titres de cette nature sont diffusés par la presse en ligne attestant d'une possible exacerbation des tensions entre les différentes parties en conflit. Le 26 février 2021 le site voaafrique.com titre: «l'armée camerounaise de nouveau accusée d'exactions contre les civils»: le 04 février 2021 reliefweb.int titre: «Cameroun: neuf civils tués dans une attaque perpétrée par l'armée»: le 24 décembre 2021, c'est le tour de tv5monde.com de titrer: «Cameroun: ces vidéos qui accusent l'armée de massacre des civils» ou «Cameroun: un jeune torturé par les forces de défense et de sécurité en zone anglophone», etc.

Les faits ci-dessus, traités de manière brute, donnent raison aux organisateurs de ce colloque qui pensent que les médias en ligne, par leur manière de présenter et de traiter l'information, contribuent à exacerber les tensions et l'insécurité dans les différentes zones de conflit. Tout ceci nous rappelle la France de l'époque révolutionnaire où la publication des «petites feuilles» s'est répandue tout en sombrant en peu de mois dans le fanatisme, le terrorisme et des appels aux meurtres[5]. Le sociologue Valentin Nga Ndongo fait une analyse pareille sur la presse camerounaise des années 1990 lorsque la communication sociale a été libéralisée mettant un terme au régime d'exception en vigueur depuis 1962. Pour lui, les contenus des journaux camerounais faisaient apparaître de l'information spectacle qui est une information truquée et mensongère dans laquelle la mise en scène l'emporte sur la réalité, le vrai se conformant à des règles fausses. C'est une information qui est destinée plus à frapper l'imagination, à appâter le public, qu'à lui apporter des éléments de connaissance[6].

Concernant les médias en ligne, les dérives notamment sécuritaires qui sont observées trouvent leur fondement notamment dans le fait que l'on est en présence d'un mode de communication où l'on retrouve des «non-journalistes», des experts, et peut-être beaucoup plus les internautes de base. A côté des sites d'information disposant d'une rédaction jouant un véritable travail éditorial, l'on a des sites participatifs dont le rôle des journalistes se limite à la validation et la mise en ligne des contributions des internautes. A cela il convient d'accorder une attention à ce que Jean-Marie Charon appelle l'organisation des rédactions qui coïncident

[5] M. Rodet, Pluralisme et diversité des opinions dans les médias, Autres temps, 1987, p: 31.
[6] V. Nga Ndongo, «Médias au Cameroun: mythes et délires d'une société en crise», Paris, l'Harmattan, 1993.

avec les principaux types de stratégies éditoriales. Pour lui, l'organisation des sites offrant une information instantanée, à jet continu, donne une place assez centrale à un desk de journalistes capables de traiter le plus rapidement possible les nouvelles directement issues des agences. Et aux côtés du desk «s'articulent des pôles chargés du développement de l'actualité par grands domaines, ainsi que des ateliers spécialisés (studios vidéo, etc.)»[7].

Toutefois, les médias qu'ils soient classiques ou en ligne peuvent aussi jouer un rôle positif dans un contexte d'insécurité ou de conflit par leur capacité et leur manière de diffuser des informations et des images qui peuvent susciter la compassion et attirer l'opinion publique à la faveur des forces de défense et de sécurité, ou au profit d'une cause noble. La presse en ligne peut également, comme tout producteur de discours, faire des mises en récit, *storytelling*, qui peuvent émouvoir le public, et donc retenir son attention et le convaincre de la justesse d'une cause. Par cette démarche, elles rompent le monopole que peuvent avoir les autorités publiques dans le traitement de l'insécurité et la construction du discours sur la sécurité. En France, c'est la presse à grand tirage qui met sur la place publique l'affaire Dreyfus et sera «l'instrument d'une historique victoire de la justice». C'est également elle qui dévoile les horreurs du bagne de Cayenne qui sera fermé ensuite, ou encore la persistance de l'esclavage[8]. L'on a pu l'observer en 1999 lors de la guerre au Kosovo avec la diffusion des images des colonnes de réfugiés utilisées comme autojustification par l'Organisation du Traité de l'Atlantique Nord (OTAN) à propos des bombardements commis sans mandat de l'ONU[9].

Le lien entre médias en ligne et insécurité devrait ainsi être pensé de façon dialectique sans parti pris, mais en considérant que les journalistes peuvent commettre des dérives susceptibles d'exacerber des tensions et mettre en péril des plans de sécurité, en même temps qu'ils sont des coproducteurs du discours sur la sécurité, et peuvent être utiles pour multiplier les regards sur un conflit et permettre d'éviter la manipulation de l'information. Dans ce cas, quelle perspective serait envisageable dans le rapport entre médias en ligne et sécurité dans le contexte de nouvelle gouvernance qui compte dépasser une vision statique et stato-centrée de la sécurité?

---

[7] J.-M., Charon , De la presse imprimé à la presse numérique. Le débat français», dans Réseaux, 2010, n°160-161, p: 24.
[8] M. Rodet, Ibid.
[9] A. Mercier, Quelle place pour les médias en temps de guerre ? Pour le titre original: «Guerre et médias: permanences et mutations», Raisons politiques, n°13, février 2004, pp: 97-109.

Le cadre théorique pertinent nous permettant de donner une réponse à notre questionnement est celui des approches pluralistes ou critiques de la sécurité, celles-là qui vont au-delà des autorités de l'Etat et qui tiennent compte des processus de recomposition et de transformation qui traversent le champ de la sécurité depuis la fin du système bipolaire, et l'émergence d'acteurs de plus en plus nombreux s'intéressant légitimement à la sécurité des sociétés. Ces approches s'intéressent principalement non pas aux faits d'insécurités, mais à la construction du discours sécuritaire. Elles émergent dans les années 1990 avec pour fil conducteur l'idée selon laquelle les études de sécurité sous l'ère bipolaire basée sur un raisonnement stratégique, étaient réfractaires au tournant autoréflexif proposé par des auteurs comme Cox et Ashley en 1981[10]. Contre Thomas Hobbes et en lieu et place d'une conception militariste et stato-centrée, certains auteurs dont les plus connus sont Krause et Williams, soutenus ensuite par les sociologues, anthropologues, féministes, etc. proposent de penser la sécurité au-delà de cette conception statique que veulent reprendre les organisateurs de ce colloque, pour «un élargissement du répertoire d'actions des pratiques de sécurité au-delà de l'instrument militaire»[11]. C'est dans cette foulée que Didier Bigo demande de prendre au sérieux les conditions de production des discours dominants sur la sécurité et les faiblesses intrinsèques des analyses réalisées selon les canons traditionnels du réalisme. Dans ce cas il est question de dépasser les perspectives réalistes et néo-réalistes qui envisagent la sécurité sur le prisme des seules autorités politiques de surplomb et dans le cadre du contrat entre l'Etat et le citoyen, seul espace pertinent dans lequel une coordination efficace de l'action collective est réalisable[12]. C'est cette vision pessimiste, instrumentale et hobbesienne qui est partagée par les Etats africains mais qui demande à être appréhendée de manière critique, car le discours sur la sécurité est un discours pluraliste coproduit par une multitude d'acteurs dont il faut s'intéresser si l'on veut avoir une vision «réaliste» de la sécurité. Didier Bigo reconnaît qu'Albert Hirschman dans *Deux siècles de rhétorique réactionnaire (1990)*, avait déjà examiné «l'argumentaire de la mise en péril» et la «justification de l'exceptionnalité des mesures antisubversives», tout comme Michael Rogin, à propos du maccartisme, a insisté sur «la fabrication de l'inquiétude par les discours politiques, et a mis en évidence l'existence d'une tradition contre

[10] G. Bertrand et M. Delori, Etudes critiques de sécurité, Etudes internationales, vol. 46, numéro 2-3 juin-septembre 2015, p: 139.
[11] B. Buzan cité par Gilles Bertrand et Mathias Delori, 2009, ibid.
[12] B. Delcourt, Théories de la sécurité, notes provisoires rédigées, ULB, 2006-2007, p: 25.

subversive qui [est] le fait des acteurs politiques centraux»[13]. Michel Foucault, quant à lui, a disséqué les discours du type «il faut défendre la société» pour montrer qu'ils sont liés à une certaine façon de concevoir les rapports d'identité et d'inimitié[14]. Les analyses de Murray Edelman sur la construction des figures de l'ennemi s'inscrivent dans la même perspective, et ne sont guère éloignées de celle d'Ole Waever, Jeff Huysmans et d'autres internationalistes qui ont examiné «comment s'est instauré un élargissement de la sphère de la sécurité, allant au-delà des questions de défense et incluant la sécurité de la société, les incivilités, les peurs intimes»[15].

Le discours que tiennent les organisateurs de ce colloque à l'endroit des médias en ligne relève alors des procédés rhétoriques traditionnels connus de construction de figure de l'ennemi, et de présentation du monde social en termes de danger et de risque. C'est une forme de «mise en spectacle politique des questions de sécurité» qu'il convient d'examiner de près car les médias internationaux en ligne sont au même titre que d'autres acteurs hors souveraineté, des coproducteurs du discours sécuritaire, au lieu d'être tenus en piètre estime au motif que leurs informations exacerbent l'insécurité. Cela pourrait être le cas, mais une sentence péremptoire et sans jugement doit laisser la place à une objectivation plus sereine.

La méthode retenue ici est l'analyse de contenu qui est une méthode quantitative dont le but est de classer tous les éléments d'un texte dans une série de casiers à partir d'une problématique et des hypothèses précises. A partir d'un corpus, des unités d'analyse retenues et une classification, l'on procèdera à une interprétation pour dire si oui ou non les MIELs retenus ici, coproducteurs du discours sur la sécurité au Cameroun, contribuent à exacerber l'insécurité dans les différents conflits. Nous nous sommes limités à l'examen des unités d'analyse à base grammaticale constituées de mots, les titres et des chapeaux de certains MIELs. Ainsi cinq MIELs dont le taux de pénétration est suffisamment élevé en Afrique et dont le traitement des conflits au Cameroun est assez régulier ont été retenus. Il s'agit de France 24, RFI, BBC Online, Jeuneafrique.com, et DW. Pour chaque MIEL nous avons retenu dix titres et chapeaux, soit un total de 50 titres et chapeaux sur la période allant de 2017 année du déclenchement effectif de la

[13] D. Bigo , *Comment douter de la sécurité ?* in Hommes et Migrations, n°1241, janvier-février 2003. Incriminés, discriminés, p: 36.
[14] Ibid.
[15] Ibid.

lutte armée dans le NOSO et 2022 année en cours qui est toujours caractérisée par l'insécurité dans cette région et dans l'extrême-nord du Cameroun. Dans les titres et chapeaux nous identifierons le nombre d'expressions susceptibles d'exacerber l'insécurité et utilisées par un MIEL, le nombre de fois que ces mots et expressions sont utilisés par ce MIEL, et enfin le nombre de fois que tous les MIELs utilisent ces mots et expressions. Ce qui nous intéresse dans ces titres et chapeaux ce sont les connotations des énoncés produits et les partis pris qu'ils révèlent.

Notre hypothèse est qu'il existe effectivement un lien entre certains MIELs et la production du discours sur la sécurité au Cameroun avec une possibilité d'exacerbation des tensions dans un camp ou dans un autre. Toutefois l'examen des titres et chapeaux des MIELs retenus fait ressortir autant une incrimination des forces de défense et de sécurité gouvernementales qu'une accusation à l'endroit des groupes armés non-étatiques: expression générique et quelques peu abusive qui désigne autant des acteurs privés, sans intention politique affichée, des groupes d'auto-défense fondés avec la bénédiction d'Etats en difficulté, les grands acteurs internationaux contraints de travailler dans des régions à forte insécurité,[16] ou les groupes armés ayant une réelle intention politique. Pour le cas du Cameroun, il s'agit particulièrement des combattants de la secte islamique Boko Haram d'une part, et les groupes armés sécessionnistes du Nord-ouest et du Sud-ouest d'autre part.

Cette communication contribue à la littérature sur les relations entre les médias internationaux en ligne et les FDS, avec un accent particulier sur la contribution de ces médias comme coproducteur d'un discours sécuritaire instantané mais qualifié systématiquement d' «insécuritaire» par les pouvoirs publics. Nous questionnons le lien entre les titres et les chapeaux de la presse internationale en ligne et la construction du discours sécuritaire, et tentons de théoriser les rapports entre les médias internationaux en ligne et les forces de défense et de sécurité dans une perspective de coproduction de la sécurité. Ce travail qui a une base à la fois empirique et théorique va montrer que l'on est présence de la production instantanée d'un discours sécuritaire désétatisée (I), qui nécessite de la part des FDS l'abandon de l'illusion totalitariste comme perspective d'une nouvelle gouvernance (II).

[16] P. Conesa , «Groupes armés non-étatiques: violence privées, sécurités privées» Revue internationale et stratégique, 2003/ 1, n°49, P157.

I - UNE PRODUCTION INSTANTANEE D'UN DISCOURS SECURITAIRE DESETATISE AU CAMEROUN

Le lien que les organisateurs de ce colloque établissent entre les médias en ligne et l'exacerbation de l'insécurité au Cameroun n'est pas tout à fait faux dans la mesure où à partir d'un échantillon plus ou moins représentatif des MIELs ayant une forte pénétration sur le territoire national, nous avons pu identifier un risque d'exacerbation de l'insécurité (A), et des actes de langage incriminant de façon indifférencié les forces en présence (B).

A/ UN RISQUE D'EXACERBATION DE L'INSECURITE

Le choix que nous avons porté sur les titres et chapeaux est justifié à plus d'un titre. N'est-il pas vrai que comme dans tout œuvre d'esprit ou tout écrit, le titre, accompagné de son chapeau, condense l'idée générale de la pensée ou du récit de l'auteur et favorise ou non la poursuite de la lecture par la personne qui s'en saisit. Le titre n'est pas seulement la porte d'entrée d'un ouvrage quel que soit son volume, c'est également le résumé de la pensée. C'est dans ce sens que Jacques Mouriquand affirme que 80% du contenu d'un journal est éliminé en quelques minutes de feuilletage et un mauvais titre d'un bon article peut lui faire perdre la moitié de ses lecteurs. Nous sommes en présence de l'élément le plus important d'un article, d'où la place qu'il occupe, le caractère et la taille qui lui sont dédiés. L'on parle d'un signal qui sert à inciter le lecteur à lire l'article et à l'orienter dans les rubriques et les pages. Le titre résume alors l'article et peut être considéré comme une étiquette qui renseigne sur le contenu. Le message que veut transmettre l'auteur de l'article est alors bien reçu à partir du seul titre. Nous considérons également que le titre a un statut autonome qui nous exonère de la lecture de l'ensemble de l'article[17]. Tout ceci est très bien résumé par Charaudeau quand il écrit: «les titres d'information sont d'une importance capitale: car non seulement ils annoncent la nouvelle («la fonction épiphanique»), non seulement ils conduisent à l'article («fonction guide»), mais encore, ils résument, ils condensent, voire ils figent la nouvelle au point de

[17] Ngoc Quan Tran , étude des titres de presse: classement syntaxique, valeurs sémantiques et pragmatiques, Mémoire de Master Recherche, Université de Toulon, 2016-2017, pp: 5 et s.

devenir l'essentiel de l'information. Le titre acquiert donc un statut autonome: il devient un texte à soi seul, un texte qui est livré au regard des lecteurs (et à l'écoute des auditeurs) comme tenant le rôle principal sur la scène d'information».[18]

L'exploitation des titres et des chapeaux des cinq grands médias internationaux en ligne sélectionnés nous renseignent suffisamment sur les contenus en lien avec la lutte contre l'insécurité au Cameroun et surtout le risque d'exacerbation des violences entre parties en conflit. Au lieu de se limiter aux mots, le choix a été fait de s'intéresser aux groupes de mots ayant une pertinence par rapport à notre problématique. Ainsi peut-on lire des phrases telles que: «Des combattants séparatistes anglophones ont été tués» (france24.com, 14 nov. 2018), «Cameroun: regain de tension en zone anglophone, il y a une escalade la violence» (RFI, 04 fév. 2018), «un champ de bataille entre les forces gouvernementales et les rebelles» (BBC, 19 nov. 2018), «NOSO camerounais: les jeunes sont les premières victimes d'une sale guerre» (DW, 07 nov. 2020), «l'armée camerounaise régulièrement accusée d'exactions» (jeuneafrique.com, 03 août 2021), «Bamenda: le spectre de la sale guerre» (jeuneafrique.com, 14 fév. 2021), «mini-guérilla faisant de milliers de morts»(france24.com), etc.

MIEL	**Nbre de titres ou de chapeaux ayant des mots ou groupes de mots pertinents sur une base de 10 échantillons**	**Nbre de mots ou groupes de mots pertinents dans tous les 10 titres**	**Nbre de mots ou groupes de mots pertinents dans tous les 10 chapeaux**
France24.com	7= 70%	13	14
Rfi.fr	9= 90%	3	13
Bbc.com	7= 70%	4	7
DW	6= 60%	2	4
Jeunafrique.com	9= 90%	4	9
Total	38= 76%	26= 52%	47= 94%

Source: Données collectées par l'auteur

[18] Charaudeau, 1983, cité par Ngoc Quan Tran, op, cit, p: 17.

Le tableau ci-dessus nous montre que 76% de titres ou de chapeaux ont des mots ou groupes de mots susceptibles d'exacerber la violence ou l'insécurité dans un camp ou dans un autre. Dans les différents titres, 52% de mots ou groupes de mots ont une charge émotionnelle susceptible d'amplifier la violence, et 94% de mots ou groupes de mots contenus dans les chapeaux sont également à même d'exacerber ces violences car ils mettent en avant les atrocités en incriminant soit les forces de sécurité, soit les groupes armés rebelles. L'on pourrait également établir un lien, fut-il faible, entre ce traitement de l'information par les MIELs sélectionnés avec les positions politiques de leurs Etats d'appartenance. Dans la guerre contre Boko Haram, la France aurait exigé le paiement de 50 millions de francs CFA par jour pour aider les FDS camerounaises à repérer par voie satellitaire les positions sans cesse mutantes des terroristes dans la région de l'Extrême-Nord du Cameroun. D'autres pays occidentaux sont reconnus pour avoir abrité les séparatistes ambazoniens tout en livrant armes et munitions à ceux qui combattent dans le Nord-Ouest et le Sud-Ouest du Cameroun. L'on peut également citer les tentatives de certaines grandes puissances à faire adopter une résolution au Conseil de sécurité des Nations unies pour une intervention armée au Cameroun. Le risque d'exacerbation de l'insécurité par les MIELs est réel si l'on s'en tient à notre échantillon. L'on, a par ailleurs, l'impression que certains grands médias articulent leur ligne éditoriale avec les objectifs de politique étrangère de leur Etat d'origine. Ceci confirme l'hypothèse principale retenue par les organisateurs de ce colloque qui ont une conception à la fois hobbesienne et wébérienne de l'Etat et de la violence dite légitime. Cependant, autant les FDS sont incriminées, autant les accusations sont également portées à l'endroit des groupes armés rebelles ou les terroristes du groupe Boko Haram.

B/ UNE INCRIMINATION INDIFFERENCIEE DES FORCES EN PRESENCE

Dans l'observation faite de l'usage des mots et expressions susceptibles d'exacerber l'insécurité dans le NOSO, les MIELs formulent leurs titres en s'appesantissant tant sur l'action des FDS gouvernementales que sur les rebelles sécessionnistes. Il existe un effort d'équilibre dans le traitement de

l'information qui consiste à «incriminer» la partie gouvernementale quand cela est possible pour eux, ou de pointer du doigt «les exactions» commises par les ambazoniens. A l'attention des forces de sécurité gouvernementales l'on peut lire des groupes de mots comme: «Au moins 25 «Amba boys», des combattants séparatistes anglophones, ont été tués dans des combats mardi dans la région du Nord-Ouest du Cameroun» (France24, 14 nov. 2018), «L'assassinat d'un sénateur influent, mardi, au Cameroun, pays hôte de la CAN-2022, met en lumière le conflit qui s'enlise en zone anglophone et que le gouvernement tente de dissimuler» (France24, 15 janv. 2022), «l'armée camerounaise, régulièrement accusée d'exactions» (Jeune Afrique, 3 août 2021), «Un homme met calmement feu à une maison, sous le regard d'un groupe d'au moins 12 hommes vêtus de treillis, de casques et de sangles noires, semblables à ceux portés par une unité de l'armée d'élite au Cameroun. (BBC, 25 juin 2018), etc.

Contre les séparatistes l'on peut lire des mots ou groupes de mots comme «Au Cameroun, les séparatistes détruisent notre avenir» (DW, 16 déc. 2021), «les querelles de leadership qui divisent les défenseurs de la cause anglophone» (Jeune Afrique, 19 nov. 2021), «Des hommes armés ont tué, vendredi, 22 civils, dont 14 enfants et des femmes, dans un village d'une province peuplée par la minorité anglophone dans le Nord-Ouest du Cameroun. (France 24, 17 février 2020), etc.

Parmi les différents titres examinés, l'on peut observer qu'il y en a qui sont informatifs pendant que d'autres sont incitatifs. Le titre informatif est celui qui donne en général un maximum d'information sans intention particulière de retenir astucieusement l'attention du lecteur. Jean-Luc Martin-Lagardette relève que ce type de titre contient l'essentiel de l'information et doit être précis. Il répond à cet effet aux questions principales que sont: qui (l'agent de l'action, le sujet de l'évènement), quoi (l'évènement), où et quand (les références d'espace et de temps qui permettent de situer l'évènement) ?[19] A travers ces repères l'auteur de l'article peut transmettre l'essentiel de l'information en si peu de mots et éviter des titres vagues, allusifs, intemporels, généraux. Les journalistes ayant formulé les titres des cinq organes de médias examinés peuvent parfaitement se défendre du fait qu'ils ont respecté les canons de leur

[19] Ngoc Quan Tran, op, cit, p: 26.

métier en tentant de ne fournir que l'information nécessaire à la connaissance de l'évolution des conflits. Mieux encore, ils peuvent se défendre d'avoir respecté les quatre règles de fabrication du titre informatif telles qu'Yves Agnès les a suggérées: i) répondre aux questions de référence, ii) condenser en éliminant les redondances, les mots inutiles, les compléments d'information non essentiels, iii) jouer avec la titraille et particulièrement avec le surtitre pour situer l'action ou donner le domaine concerné par l'article, iv) procéder avec ou sans verbe[20]. Toutefois, pour les FDS dont la conception du discours sécuritaire est stato-centrée, le seul fait de faire allusion dans ce qui se fait dans les zones de combat est une atteinte à la sérénité des opérations. Les médias n'ayant pas la légitimité de produire un discours sécuritaire devraient s'abstenir à défaut de présenter une version des faits favorable aux forces gouvernementales.

Le titre incitatif, quant à lui, travaille plus à retenir l'attention ou la curiosité que de fournir simplement de l'information au lecteur. S'il cherche toujours à surprendre, faire sourire, intriguer par des images audacieuses, des mots chocs, des jeux de mots ou des formules détournées, dans le cadre de cette recherche l'on est en présence des formules qui peuvent plutôt incriminer un camp et indiquer qu'il est responsable des tueries ou de l'insécurité observées. Pour Martin-Lagardette, les titres incitatifs «révèlent l'esprit de l'article plus que sa matière et s'appuient souvent sur des jeux de mots inspirés de titres de films ou de livres, de slogans publicitaires, etc.»[21]

Face aux informations diffusées par les MIELs incriminant les forces de défense et de sécurité, la réaction du gouvernement camerounais est quelque peu constante et tourne autour d'un démenti sur l'ensemble de ce qui est considéré comme des «allégations mensongères», ou l'annonce d'une enquête visant à établir les différentes responsabilités. Ceci confirme encore le regard délégitimant que les FDS portent sur les acteurs hors souveraineté comme les médias en ligne. En 2018 à la suite de la diffusion d'une vidéo sur les réseaux sociaux montrant des exactions imputées à l'armée camerounaise dans la région de l'Extrême-nord, le porte-parole du gouvernement avait promis l'ouverture

[20] Ngoc Quan Tran, op, cit, p: 27.
[21] Op, cit, p: 28.

d'une enquête visant à établir les différentes responsabilités. Ceci montre la presqu'obligation de comprendre que les médias en ligne ou classiques font partie du paysage des acteurs sécuritaires, et leur discours est pris en compte tôt ou tard. Par ailleurs, il est évident que les questions de la sécurité du Cameroun occupent une place non négligeable dans l'agenda des MIELs ou les sites web des médias classiques. Toutefois, dans la production de ce discours sécuritaire, chaque partie au conflit en prend pour son grade, et nul n'est épargné dans les accusations d'exactions, même si la balance pèse plus du côté des FDS. La présentation des faits se fait comme dans tout processus de *sécuritisation*, où le producteur du discours sur la sécurité établit une menace existentielle suffisamment saillante pour avoir des effets politiques substantiels[22]. Que les informations soient vraies ou fausses, Buzan, Waewer et Wilde soulignent l'existence d'»une forme d'instrumentalisation par la désignation d'une menace que le discours doit faire connaître comme telle»[23]. Toutefois notre analyse montre également qu'autant l'instrumentalisation est le fait des médias en ligne examiné, autant elle est le fait des FDS qui procèdent à leur tour à ce que Bigo appelle «la constitution d'une gestion symbolique des inquiétudes et des peurs (fantasmatiques ou non) qui dérivent du changement social international actuel»[24]. Dans le discours que tiennent les organisateurs de ce colloque l'on peut également y voir qu'il Il y a «construction sociale, à partir des faits précis, d'une image de l'ennemi qui n'est programmée par personne mais qui découle de la lutte des professionnels de la sécurité pour la hiérarchisation des priorités en termes de gravité des menaces et des risques»[25]. Pour éviter cette instrumentalisation de part et d'autre, la nouvelle gouvernance sécuritaire au Cameroun n'exige-t-elle pas que les FDS soient en rapport direct avec les MIELs qui participent à la coproduction du discours sécuritaire ?

II/ L'ABANDON DE L'ILLUSION TOTALITARISTE COMME PERSPECTIVE D'UNE NOUVELLE GOUVERNANCE SECURITAIRE

[22] Le Gouriellec, op, cit, p: 90.
[23] Ibid.
[24] Didier Bigo: *Comment douter de la sécurité ?* op, cit, p: 39.
[25] Ibid.

En démocratie, il vaut mieux discipliner que réguler, dialoguer que réprimer et il semble que la discipline sied mieux avec le concept de nouvelle gouvernance que veulent penser les organisateurs de ce colloque dans le cadre des relations entre les médias en ligne et les forces de défense et de sécurité au Cameroun. Si dans le domaine de l'entreprise la gouvernance renvoie aux bonnes pratiques de gestion, et dans la littérature des institutions financières internationales, elle met en évidence la bonne gestion des affaires publiques, dans les relations internationales, ce concept et sa pratique suggèrent l'idée d'une prolifération des modes de régulation, de niveaux, des instances de décision et récuse toute idée d'organisation et de contrôle centralisés[26]. Marie-Claude Smouts pense à juste titre qu'il s'agit de «donner une visibilité à des acteurs et à des interactions négligés par la littérature réaliste, et de renouveler la réflexion sur l'idée de société internationale, bien qu'elle puisse conduire à cautionner insidieusement le plus cynique des néolibéralismes»[27]. Avec l'avènement des médias internationaux en ligne et l'activité qu'ils mènent en termes de diffusion instantanée de l'information et parfois de manipulation de cette information, il faut justement renouveler la pensée sur les rapports que les forces de défense et de sécurité ont avec l'information. Il faut repenser l'idée de la «grande muette», expression issue de la IIIe République en France et qui ne peut plus garder le même sens en ce XXIe siècle caractérisé par les revendications permanentes sur les droits et libertés et la sophistication toujours permanente des moyens de diffusion et d'accès à l'information. Ceci passe au moins par la mise sur pied de mécanismes facilitant l'accès des MIELs à la bonne information d'une part (A) et la socialisation du grand public d'autre part (B).

A/ LA MISE SUR PIED DES MECANISMES FACILITANT L'ACCÈS A LA BONNE INFORMATION

Au-delà des questions de sécurité, le contexte de gouvernance mondiale nous insère dans un espace de coexistence entre les deux mondes que décrit James Rosenau et qui sont repris par Bertrand Badie: un monde des Etats,

[26] M –Cl. Smouts, «Du bon usage de la gouvernance en relations internationales», Revue internationale des sciences sociales: «*La gouvernance*», Unesco, Erès, n°155, mars 1998.
[27] Smouts M –Cl., ibidem.

codifié, ritualisé, formé d'un nombre fini d'acteurs, connus et plus ou moins prévisibles, et un monde multicentré constitué d'un nombre presqu'infini de participants dont on ne peut que constater qu'ils ont une capacité d'action internationale plus ou moins autonome de l'Etat dont ils sont censés relever[28]. Tenter d'ignorer ce monde ou de vouloir lui imposer des régulations conçues unilatéralement est désormais illusoire. En matière de défense et de sécurité et dans un contexte de conflit, plusieurs démarches peuvent être adoptées par les forces gouvernementales pour faciliter l'accès à la bonne information aux médias en ligne et éviter toute manipulation de l'information pouvant entraîner une exacerbation de la violence dans un camp comme dans un autre.

Les perspectives d'une stratégie de communication efficace renvoient en somme aux bonnes pratiques tant au plan interne, au plan externe, et au niveau de la communication opérationnelle mobilisant Internet et les réseaux sociaux comme moyens modernes pour expliquer aux séparatistes du NOSO par exemple le bien-fondé de l'abandon des armes, et aux populations les avantages d'une collaboration avec les forces gouvernementales[29]. Si le Web est complémentaire aux voies classiques d'information et de communication que sont la radio, la télévision et la presse écrite, son usage devrait néanmoins répondre à une stratégie plus offensive tant au plan politique, qu'au niveau opérationnel.

Aussi, une stratégie adaptée de communication en ligne serait-elle suivie par la systématisation des comptes rendus d'opérations, et la formation des personnels de communication des forces de défense et de sécurité à la communication en ligne.

- LA STRATÉGIE DE COMMUNICATION EN LIGNE ADAPTÉE

La première étape du changement de l'ordre communicationnel existant au sein des FDS camerounaises consiste à élaborer une stratégie adaptée de communication numérique dédiée. Cette stratégie devrait être une sorte de

[28] Badie et Smouts: «Le retournement du monde. Sociologie de la scène internationale», 3e édition, Presses de Sciences Po et Dalloz, 1999, p 66.

[29] Certaines études s'intéressent également à la communication de recrutement.

cahier de charges à l'attention des communicants des FDS alliant exigence du secret des opérations à mener et utilisation adéquate des moyens modernes de communication que sont Internet et les réseaux sociaux. Il est question d'élaborer, puisqu'elle n'existe pas encore, une stratégique de communication globale précise, car la communication sur les réseaux sociaux et cette stratégie globale sont intimement liées, celle-là découlant de celle-ci. Cette communication globale est elle-même le produit d'une stratégique générale, qui si elle n'est pas claire, rendra la tâche des communicants difficile, notamment pour identifier les messages à faire passer que ce soit sur Internet ou sur d'autres supports[30].

- LA SYSTÉMATISATION DES COMPTES RENDUS D'OPÉRATION

La lutte contre la Covid-19, considérée comme une crise majeure dans tous les Etats au monde, a révélé non seulement la capacité de résilience qu'ont les petits Etats, mais aussi la possibilité qu'ont les gouvernements à rendre compte au quotidien des actions qui sont menées en faveur des populations. Depuis l'avènement de la crise au Cameroun, le citoyen a droit quotidiennement, lors du journal télévisé de 20h30 à la télévision nationale (CRTV), d'un compte rendu des opérations de lutte contre la pandémie donnant les chiffres et les nouvelles mesures prises par le gouvernement pour éradiquer ou au moins faire reculer la maladie. Cet exemple de transparence et de respect du citoyen ne peut-il pas être adopté dans le cadre de la lutte contre les autres formes d'insécurité ?

Par ces temps de démocratie et de transformation des pratiques des conflits, tout acteur chargé de tenir un discours sur la sécurité, quelle que soit sa place dans la hiérarchie, quel que soit son emploi, doit être autorisé et capable à son niveau de rédiger un compte rendu ou un rapport circonstancié sur une opération de sécurité.

Plus sommaire que le rapport d'un fait ou d'une situation, le compte rendu dans le cadre d'une opération militaire ou de sécurité s'emploie classiquement

[30] Marck Hecker, Nicolas Vanbremeersch, Marguerite de Durand et Thibault Souchet: Nature et conséquence des réseaux sociaux pour les forces armées, IFRI, septembre 2012, p: 111.

pour signaler à l'autorité supérieure soit l'exécution d'une mission ou d'un service, soit un fait de peu d'importance, soit un évènement grave que l'autorité doit connaître sans délai, en attendant la venue d'un rapport circonstancié[31]. Au-delà du rapport hiérarchique dans lequel il s'inscrit traditionnellement et qui limite sa diffusion, un compte rendu d'opération tel que nous l'envisageons ici est une démarche de communication interne et beaucoup plus externe consistant à faire le point sur une opération dans un secteur donné pour une période bien déterminée sur la base des objectifs qui ont été clairement définis à l'avance. Le but est d'évaluer la situation et les besoins qui peuvent contribuer à l'amélioration de l'état des choses et de porter à la connaissance du public les informations nécessaires.

Le compte rendu d'opération, en plus d'être confondu avec la communication institutionnelle, ne semble pas être systématique et formalisé au sein des forces de défense et de sécurité camerounaises. La communication institutionnelle que mène le chef de division de la communication qui est directement rattaché au ministre délégué chargé de la défense est différente de la communication opérationnelle qui est une fonction opérationnelle relevant logiquement du chef d'Etat-Major des Armées (CEMA). A juste titre car dans la plupart des pays, le CEMA est responsable de la planification, de la préparation et du déploiement des forces armées sur le terrain. Il dispose à cet effet d'un état-major et s'appuie sur un quartier général pour les opérations interarmées. C'est normalement à lui ou à ses services qu'il revient de produire et de présenter ces comptes rendus d'opération[32]. A des moments cet exercice est effectué lors des descentes sur le terrain du CEMA dont les missions sont des missions d'opération. Sous forme de déclaration sommaire à la presse, des informations sont souvent données sur l'objectif de la mission et le sentiment par rapport à l'application des mesures dictées par la hiérarchie. C'est le cas à de multiples reprises à l'exemple de la mission de contrôle opérationnelle effectuée en janvier 2021 à la frontière Cameroun-République centrafricaine, ou lors de la mission de contrôle opérationnelle effectuée en juillet 2020 dans

[31] Ministère de la Défense: La correspondance militaire, Etat-Major de l'Armée de Terre française, édition provisoire 2001, p: 19 et s.

[32] En France c'est l'Etat-Major des Armées (EMA) qui est en charge de la communication opérationnelle. Pour s'arrimer à la nouvelle donne de communication, elle ouvre son premier compte Twitter en novembre 2015, 10 jours après les attentats de Paris.

les régions militaires interarmées n°2 et n°5 à Buea, Bamenda et Douala. A l'issue de la mission, une rencontre à huis clos est tenue avec d'autres hauts responsables des FDS, et suit une déclaration à la presse avec des mots à peu près similaires: «je suis descendu sur le terrain effectuer des contrôles opérationnels pour m'assurer que la situation est bien en main et que nos hommes n'ont pas de problèmes particulier»[33].

Les comptes rendus d'opération permettraient ainsi de réduire les effets de la propagande de guerre menée par le camp adverse et exploitée par les médias en ligne en manque d'informations provenant des états-majors. Qu'ils soient classiques ou cybernétiques, les médias sont reconnus pour leur contribution dans une société démocratique, y compris en matière de sécurité et de défense. Mais cette contribution n'aura de sens que si les autorités publiques se délestent de l'idée de censure et font bénéficier aux médias d'une véritable liberté, d'une indépendance effective, et mettent à leur disposition de la bonne information. D'aucuns estiment que le jeu démocratique «reste tributaire de cette liberté de presse et la démocratisation du secteur de la défense et de la sécurité n'échappe pas à cette logique. Un cadre légal à travers un code de communication ou son équivalent, un groupement syndical ou un ordre des journalistes sont nécessaires pour protéger les gens des médias dans l'exercice de leur travail, particulièrement dans un domaine aussi sensible que la politique de sécurité et de défense»[34].

- LA FORMATION DU PERSONNEL MILITAIRE À LA COMMUNICATION NUMÉRIQUE

La formation est le volet interne de la nouvelle gouvernance que pourrait mettre sur pied les forces de défense et de sécurité dans leurs relations avec les médias en ligne dans la mesure où elle vise à renforcer les capacités des officiers et sous-officiers afin qu'ils maîtrisent eux-mêmes la diffusion des informations en complément de ce que font les médias publics. Cette formation en permettant aux personnels de défense et de sécurité de mieux maîtriser les TIC, permet également de corriger à chaque fois les manipulations

[33] Cameroon-Tribune.cm publié le 20 juillet 2020 à 12: 11.
[34] Friedrich-Ebert-Stiftung: *Sécurité et défense: Nouveaux défis, nouveaux acteurs*, Antananarivo, 2009, p: 34.

d'information qui prolifèrent dans certains médias en ligne. De nombreuses analyses ont montré combien les médias sociaux sont habités presqu'au même titre que les médias traditionnels ou avec leur complicité par la propagande et la diffusion d'images ou de vidéos falsifiées ou sorties de leur contexte pendant les périodes de conflits[35]. L'objectif recherché serait le même en l'occurrence: diaboliser l'adversaire, attirer la sympathie de l'opinion publique internationale en «pinçant la corde sensible», fabriquer le consentement de l'opinion publique, justifier l'intervention étrangère[36].

En formant le personnel des forces de défense et de sécurité à l'usage de la communication numérique cela permet, au-delà de vouloir compléter le travail des médias publics, d'utiliser parfois les mêmes armes que mobilisent les groupes armés rebelles.

Dans l'insécurité qui sévit dans le NOSO, la radicalisation des leaders de la minorité anglophone a été amplifiée par l'usage du Web 2.0 qui leur offre une interactivité et toute la simplicité d'utilisation, en leur permettant de se faire entendre tant par leurs adeptes, par le gouvernement, que par la communauté internationale. Présentées sous forme de «nationalisme de libération», ces revendications anglophones, révélatrices d'une nouvelle forme d'activisme, se sont facilement diffusées et ont favorisé une action collective sans précédent grâce à Internet et aux réseaux sociaux. Résidant en Afrique du sud, en Europe ou en Amérique du Nord, les leaders séparatistes anglophones du Cameroun ont su utiliser le numérique comme outil de mobilisation afin de mettre en mouvement une somme d'individualités autour d'une revendication qui s'est muée en conflit, alors qu'il y a quelques années, leurs mots d'ordre ne prospéraient guère et s'éteignaient aussitôt qu'ils les déclenchaient. Pas moins de douze forums de propagande sécessionnistes ont été créés par les séparatistes du NOSO. La grande mobilisation nationale et internationale qu'ont réussie ces leaders auprès des grandes puissances comme les Etats-Unis, la France, l'Allemagne ou la Grande-Bretagne grâce à Internet, exige que l'on s'interroge sur l'efficacité des moyens classiques de communication et de

[35] J-J. Bogui et C. Agbobli, «L'information en périodes de conflits ou de crises: des médias de masse aux médias sociaux numériques», Communication, technologies et développement [En ligne], 4 | 2017, mis en ligne le 04 juillet 2017, consulté le 29 mars 2021. URL: http:// journals.openedition.org/ctd/705; DOI: https://doi.org/10.4000/ctd.705.
[36] ibid.

propagande que les Etats utilisent encore dans la lutte contre les insécurités et les instabilités, alors que les adversaires des institutions publiques eux sont à l'ère du militantisme et de l'activisme en ligne. Cette forme d'activisme a transformé Internet et les réseaux en nouvel espace public que d'aucuns qualifient d' «espace de contrôle public», «outil de surveillance étatique», «instrument d'une démocratie de surveillance»[37], et qui est pour les séparatistes anglophones du Cameroun un adjuvant stratégique ou un accélérateur de propagande.

Les éléments ci-dessus développés concernent la pleine appropriation d'Internet et des réseaux sociaux par le renforcement des capacités des sous-officiers spécifiquement chargés d'alimenter les pages web et d'envoyer les liens vers les populations cibles et les médias. La spécialisation des sous-officiers permet de mieux préserver la ligne de démarcation entre ce qui doit être publié et ce qui relève du secret des Forces armées. Mais elle peut également être substituée par une solution similaire à celle qu'adopte la France qui fait appel à des prestataires privés pour créer et alimenter la page Facebook du ministère de la Défense. Non seulement Internet génère de l'impatience et donc oblige à avoir une équipe qui y travaille en permanence, en plus cette équipe doit être spécialisée dans la grammaire du Web, notamment savoir expliquer en quelques lignes, voire en quelques dizaines de signes, les raisons et les objectifs d'un déploiement. L'on sait que si sur Twitter l'on ne répond pas à un message dans les minutes qui suivent sa réception, la réponse peut passer inaperçue, voire incongrue[38].

B/ LA SOCIALISATION DU GRAND PUBLIC

Les acteurs de lutte contre l'insécurité au sein des médias en ligne peuvent également s'inspirer de ce que font les acteurs de la lutte contre les discours haineux à travers les espaces médiatiques numériques. Ces organisations qui sont pour la plupart des acteurs hors souveraineté mènent des campagnes de sensibilisation et d'éducation à l'utilisation des réseaux sociaux pour tordre le

[37] Lassané Yameogo, "Activisme en ligne et transformations sociopolitiques au Burkina Faso", *Communication* [Online], vol. 37/2 | 2020, Online since 07 September 2020, connection on 11 October 2021. URL:http://journals.openedition.org/communication/13232; DOI: https://doi.org/10.4000/communication.13232

[38] Op, cit, p: 132.

coup à la haine et maintenir le sentiment d'inséparabilité au sein de la société camerounaise. Elles procèdent par la diffusion des récits positifs, comme l'amour, la cohésion sociale, la tolérance et le respect mutuel dans de nombreux espaces numériques comme Facebook, Twitter, Instagram, WhatsApp, etc[39]. La sensibilisation fait partie du discours sur la sécurité. Elle permet aux forces de défense et de sécurité de tenir à l'endroit des populations des messages sur la crédibilité des informations et des sources de ces informations. Tout en reconnaissant que les médias en ligne participent à la coproduction du discours sur la sécurité, il est question d'informer l'opinion sur les sources fiables contrairement à celles dont le seul but est d'exacerber l'agitation sociale et d'attiser les conflits. Cela passe une fois de plus par une présence permanente des forces de défense et de sécurité dans les réseaux sociaux afin d'utiliser les mêmes canaux qu'utilisent les entrepreneurs d'insécurité.

Malgré l'horreur que cela peut représenter pour le commun des mortels, le scénario est désormais connu dans l'usage stratégique d'Internet par les séparatistes camerounais dans leurs affrontements avec les FDS. Une fois l'alerte donnée par l'un de leurs informateurs sur une arrivée éventuelle des FDS dans leurs campements, un piège est posé et filmé par vidéo, et dès que l'Armée tombe devant eux, une autre vidéo est faite avec force de détails sur les exactions commises. La vidéo est ensuite largement diffusée avec en fond sonore des voix qui jubilent sur la réussite de l'embuscade. Toutes les violences, intimidations, assassinats et enlèvements sont ainsi filmées et diffusées en boucle sur les réseaux sociaux juste quelques minutes après la réalisation de l'opération. Une pratique particulièrement prisée par un certain «Général No Pity» connu pour son extrémisme et son habileté à pouvoir échapper aux FDS avec ses hommes, et à réapparaître quand bien même ils ont été annoncés plusieurs fois par les médias comme ayant été capturés. Toutes les occasions sont des opportunités pour les séparatistes de diffuser via Internet leurs actions et manifestations, comme c'est le cas chaque année à la date du 1er octobre considérée par eux comme le jour anniversaire de l'Etat d'Ambazonie. Ces images de manifestations sont également accompagnées de discours politiques sur la détermination à séparer les deux régions du Nord-ouest et du Sud-ouest de l'ensemble du territoire national.

Deux principaux objectifs sont poursuivis par les séparatistes anglophones dans leur usage stratégique du Web 2.0, que ce soit dans la diffusion des images

[39] DW Hate Speech FAQ https://p.dw.com/p/1I9ku consulté le 05 avril 2022 à 12h 44.

de guerre que lors des manifestations à caractère purement politique. L'un porte sur la captation de la sympathie de l'opinion publique nationale et surtout internationale pour qu'elle considère l'Armée camerounaise comme étant en position d'agresseur, et qu'elle voit en elle une Force d'occupation, comme jadis les combattants du Biafra au Nigeria considéraient l'Armée fédérale de leur pays lors du conflit civil qui se déroula entre 1967 et 1970. Cette diabolisation des FDS supposerait alors une intervention internationale susceptible de libérer le territoire occupé. L'autre objectif poursuivi par les sécessionnistes anglophones dans l'usage permanent du Web est l'humiliation des FDS gouvernementales par la diffusion de leurs défaites, et l'exhibition de leurs armes, munitions et uniformes comme butins de guerre. Cette humiliation signifierait que l'Armée camerounaise est sous équipée, mal entraînée et incapable de venir à bout de petits groupes politico-militaires. Ce qui est bien évidemment faux.

Education, participation et autonomisation des couches vulnérables, et surtout médias et coalition en ligne sont des pistes à explorer pour compléter l'action du soldat, surtout dans le cadre des conflits internes dont il est important d'éviter les séquelles post-conflit. Une communication stratégique peut efficacement aider à renverser la tendance à l'endroit des populations et des combattants rebelles. Les FDS camerounaises devraient bien profiter de l'arsenal numérique disponible pour faire passer régulièrement des messages sur l'abandon de la lutte par les sécessionnistes, et de diffuser rapidement leur version des faits en cas d'incident. Cette attitude sera en résonnance avec les stratégies modernes de communication dans les armées. L'Armée israélienne qui est censée entraîner les unités d'élites des FDS camerounaises est par exemple très branchée stratégiquement sur les réseaux sociaux. Tsahal met fréquemment en ligne des vidéos de ses opérations sur sa chaîne YouTube, et les liens sont ensuite «tweetés» et parviennent instantanément aux milliers de personnes dont de nombreux journalistes. L'on pense que YouTube permet à cette armée de contrer rumeurs et tentatives de désinformation visant à jeter le discrédit sur ses opérations[40]. De nombreuses grandes puissances limitent la régulation d'Internet à leurs personnels civils et militaires au lieu de se permettre de contrôler le monde des médias dont on sait que la liberté est au cœur de leur action. C'est ce que prévoit par exemple le Ministère de la Défense britannique (MoD) qui a publié en août 2007 une directive ayant trait à la communication et intitulée «Contact with the Media and

[40] M. Hecker et T. Rid, «Utilisation et investissement de la sphère Internet par les militaires», Etudes de l'IRSEM, 2012, n°13, non paginé.

Communicating in Public», document plus connu sous l'appellation 2007DIN03-006. Cette directive se limite à exiger aux fonctionnaires civils du MoD et aux membres des forces armées d'obtenir une autorisation préalable s'ils veulent écrire, parler ou communiquer publiquement d'une autre manière sur la Défense ou des sujets corrélés[41]. Il en est de même de l'*US Army* qui dans ses règles de sécurité opérationnelles adoptées en 2005 (Army Regulation 530-1, version 2005) se limite à demander à tous les personnels de l'*Army* de consulter leur supérieur hiérarchique et un officier de sécurité avant de publier des informations qui «pourraient contenir des données sensibles et/ou critiques sur un support publicce qui inclut mais ne se limite pas aux lettres, aux e-mails, aux sites web, aux web logs (blogs), aux discussions sur les forums d'information sur Internet»[42]. La France quant à elle met l'accent sur la sensibilisation plutôt que sur la surveillance et l'interdiction. Cette sensibilisation concerne le personnel civil et militaire de l'Armée. L'attention est portée exclusivement sur les personnels de la défense avec des règles strictes en matière de communication via Internet et les réseaux sociaux. L'état-major des armées encadre scrupuleusement chaque post. L'envoi d'un tweet ou d'un message Facebook suit le même circuit de validation que n'importe quel canal de communication et dépend bien évidemment de la sensibilité de l'information fournie. Si les images diffusées proviennent des vidéastes et des photographes de l'armée de Terre, de la Marine nationale, de l'Armée de l'Air et de l'ECPAD (Etablissement de Communication et de Production Audiovisuelle de la Défense), leur publication remonte obligatoirement par la chaîne des opérations. Elle doit être validée au plus haut niveau de l'état-major des armées. Par contre, nulle part il n'est alors question de répertorier, voire de ficher les médias publics et privés pour envisager éventuellement une régulation qui ne saurait être tolérée ni par les médias eux-mêmes, ni par l'opinion publique, malgré que l'on soit en présence des questions de sécurité et de défense. Cette régulation qui va ensemble avec un certain discours sécuritaire incriminant les médias en ligne comme producteur de l'insécurité est-elle vraiment capable de diminuer l'insécurité ou alors créé elle-même un dilemme de sécurité intérieure, comme l'on a un dilemme de sécurité internationale ? Autrement dit, le fait de vouloir restreindre la diffusion d'informations sur les opérations de l'armée ne crée-t-elle pas une insécurité du côté des médias en ligne qui, à leur tour, vont également renforcer leurs moyens

[41] M. Hecker et T. Rid, op, cit.
[42] Op, cit.

d'accès et de diffusion de ce type d'information et nuire effectivement les FDS dans leur lutte contre l'insécurité ? Didier Bigo pense que le discours sur la sécurité peut produire de l'insécurité «à travers des prophéties autoréalisatrices, où les ennemis virtuels qu'ils désignent réagissent à la stigmatisation et deviennent par moment bien réels, ce qui justifie ces discours a posteriori».

CONCLUSION

Qu'on s'entende bien, douter de la régulation des médias et demander que les FDS leur fournissent de la bonne information parce qu'ils sont des co-producteurs du discours sur la sécurité, ne fait en rien de cette communication un propos de libertaire, ou de libéral radical. L'on penserait également qu'il s'agit d'une réflexion d'une gauchiste qui critique l'ordre établi et le monopole que l'Etat dispose sur certaines questions de souveraineté. Il ne s'agit en rien de prôner le libertinage des médias et leur exacerbation de l'insécurité. L'auteur de ces lignes est un penseur de la réalité qui reconnaît que la liberté d'expression est le socle d'une démocratie qui marche, et qu'à l'ère du tout-cyber (cyberdémocratie, cyberrevendication, cyberactivisme, cyberguerre…) est-il encore possible pour les gouvernants de contrôler l'information y compris en période d'insécurité, de troubles sociaux, ou de conflits armés internes ou internationaux ? Il est évident qu'une information non-maitrisée met à mal la réussite des opérations de sécurité et peut aggraver une situation sécuritaire déjà précaire. C'est ce qui justifie, y compris dans les Etats dits démocratiques, la propension qu'ont les pouvoirs publics à contrôler la diffusion de l'information et à se rassurer que la communication est faite en leur faveur. Ceci est une fonction gouvernementale à part entière dédiée à un ministre qui est en charge de la communication gouvernementale ayant à sa disposition les médias dits de service publics, et d'autres médias dont on a bien l'impression qu'ils reçoivent des faveurs en contrepartie de leur bienveillance à l'égard de l'action gouvernementale. Mais l'action sur les médias dits de service public et ceux qui leur sont proches n'est pas suffisante à garantir aux pouvoirs publics la sérénité de leur action. D'où le recours à la censure où au moins au contrôle de l'information diffusée par les médias soit qui se disent «indépendants», soit ceux qui ne reçoivent pas de soutiens particuliers de la part des gouvernants. A l'heure d'Internet et de toutes les technologies de l'information et de la communication tout devient très difficile pour qui veut réguler l'espace public au sens habermassien du terme, c'est-à-dire

contrôler le cadre social dans lequel s'effectue sans les entraves de la censure une communication libre[43].

Les vertus que l'on reconnaît aux médias en ligne sont nombreuses et plusieurs d'entre elles sont fondées et rendent difficile la mise en œuvre de l'idée de les réguler ou de les censurer. Ils ont augmenté les opportunités offertes aux citoyens d'avoir accès à l'information instantanée et à moindre coût, d'exprimer leurs opinions, de se tenir au courant des faits les plus insoupçonnés, voire de faire concurrence aux professionnels de l'information[44]. L'on estime même que leur rôle ou au moins leur présence est incontournable en période de conflit et le pouvoir des gouvernements de les censurer s'en trouve considérablement réduit[45]. La tentative du Gouvernement de suspendre Internet dans les régions du Nord-ouest et du Sud-ouest a laissé la place à des condamnations internationales qui ont fini par le faire plier. Toute démarche de cette nature est désormais vouée à l'échec tant elle expose les gouvernements à des critiques internationales qu'ils supportent à peine, sachant qu'elles compromettent leurs chances de coopération avec les Etats dits démocratiques.

La question légitime qu'il convient de poser à la conclusion de ce travail et qui met en perspective la médiacratie cybernétique et les menaces sécuritaires est celle de savoir si les moyens classiques d'information, de communication et de propagande déployés par les FDS camerounaises face aux entrepreneurs d'insécurité sont toujours efficaces alors même que tous les acteurs recourent de façon stratégique au numérique ? Notre hypothèse pour ouvrir le débat à d'autres discussions est que ce ne sont pas les médias en ligne qui font vraiment problème, mais c'est la manière dont les forces de défense et de sécurité communiquent et conçoivent le discours sécuritaire qui est à repenser. A l'heure où l'information est devenue un enjeu stratégique dans toutes les guerres, conflits, crises et autres troubles sociaux, l'usage du numérique doit être au cœur des stratégies. L'efficacité des moyens classiques d'information, de communication et de propagande auxquels recourent encore certaines forces de défense et de sécurité est désormais limitée. Ces moyens classiques nécessitent d'être repensés dans le sens d'un renforcement des capacités offensives et défensives de communication,

[43] J. Habermas, L'espace public: Archéologie de la publicité comme dimension constitutive de la société bourgeoise, Paris, Payot, 1993, cité par Zineb Benrahhal Serghini et Céline Matuszak: «Lire ou relire Habermas: lectures croisées du modèle de l'espace public habermassien», Études de communication [En ligne], 32 | 2009, mis en ligne le 01 juin 2011, consulté le 10 décembre 2020. URL: http://journals.openedition.org/edc/868: DOI: https:// doi.org/10.4000/edc.868.

[44] J-J. Bogui et C. Agbobli, op, cit, p: 7.

[45] Ibid.

avec Internet et les réseaux sociaux comme leviers opérationnels susceptibles de créer des interactions avec le citoyen, tout en délégitimant le discours des entrepreneurs d'insécurité.

Dès le début des revendications socio-politiques et le déclenchement de la lutte armée, Internet a été pour les sécessionnistes le principal moyen de mobilisation des troupes, de transfert financier et surtout de captation de l'attention de la communauté internationale dont certains acteurs majeurs ont été pointés du doigt comme étant des soutiens politiques et logistiques avérés des séparatistes.

Les FDS camerounaises ont donc franchi le pas du *social media presence* mais ont du mal à passer au *social media engagement* car elles ne sont pas suffisamment tournées vers l'échange avec les tiers et surtout avec les sécessionnistes pour les convaincre d'abandonner la lutte. Ignorent-elles de quelle utilité l'échange avec les tiers peut également favoriser la collecte des renseignements pour leurs opérations ? Lors de la guerre de l'OTAN en Libye, le porte-parole de l'*Opération Unified Protector* a relevé combien des tweets adressés à son équipe par des Libyens permettaient de constater en temps réel le positionnement des troupes du Colonel Mouammar Kadhafi. Des quatre niveaux qui peuvent être distingués en matière d'activité institutionnelle sur les réseaux sociaux, la première étape qui est l'émission unique et unilatérale des informations est bien maîtrisée. Il reste de franchir les trois autres niveaux que sont: répondre aux internautes sur des sujets faciles, répondre à toutes les questions y compris les plus difficiles, et mobiliser des soutiens ou initier des projets collaboratifs.

De la conception hobbesienne et wébérienne de la sécurité développée dans le monde westphalien, il est tant d'envisager la nouvelle gouvernance sous le prisme d'une coproduction du discours sur la sécurité au Cameroun. Le monopole étatique et la position de surplomb qu'adoptent les gouvernements face aux questions de sécurité ne prospèrent plus depuis longtemps face à l'émancipation des acteurs hors souveraineté et au développement sans cesse croissant du numérique qui offre une information instantanée difficile à contrer. La meilleure solution est de coopérer avec tous ceux qui comme les MIELs la coproduisent. La presse est un enjeu de guerre dans la mesure où sa présence dans les lieux de conflits intéresse au premier chef les belligérants qui ont compris son rôle. Inutile de vouloir la museler et de lui nier la légitimité de produire un discours sur la sécurité. Il faut coopérer avec elle et lui faciliter la vie.

LE DEVELOPPEMENT DU CYBERESPACE ET L'IMPERATIF DU RENFORCEMENT DES CAPACITES STRATEGIQUES ET OPERATIONNELLES DES ACTEURS

Pierrette Annie EVINA, Ph.D
Directeur de la sécurité des réseaux et des systèmes d'informations, MINPOSTEL

RESUME

L'évolution des Technologies de l'Information et de la Communication (TIC) et de l'internet, ces dernières années, a favorisé la montée en puissance de plusieurs formes de criminalité numérique. De nombreux conflits et les attaques de tout genre sont fréquents sur le cyberespace et les conséquences de ces cyber-attaques peuvent s'avérer désastreuses pour les citoyens et les institutions et être préjudiciables pour la souveraineté du pays. Il est primordial de mener une lutte acharnée contre les cybercriminels et optimiser la gestion de la sécurité numérique par l'amélioration des capacités institutionnelles, organisationnelles, juridiques, règlementaires et humaines pour asseoir les stratégies de riposte aux attaques et être capable de répondre énergiquement en cas d'attaque.

INTRODUCTION

Le domaine des Technologies de l'Information et de la Communication (TIC) est actuellement au cœur de la croissance et de la compétitivité avec son lot d'opportunités. Grâce au développement de la technologie et du monde numérique, il y a au fil des années, de nombreux changements de paradigme dans la société. Plus qu'une évolution, nous vivons une révolution.

Ces dernières années notamment, les TIC ont connu un développement fulgurant avec la généralisation de l'Internet et l'utilisation croissante des données numériques qui s'en suit. Cette démocratisation de l'Internet a favorisé la montée en puissance de plusieurs formes de criminalité numérique, dans le monde entier et au Cameroun en particulier, au point où ce phénomène impacte sérieusement le quotidien de tous.

L'espace de communications numériques est aujourd'hui un terrain de compétition et de conflictualité entre les hommes et entre les nations tout comme sur terre, sur mer, dans l'air. En effet, Les individus, les entreprises et les infrastructures connectés sur Internet, sont confrontés à de nombreux types d'attaques. Celles-ci peuvent varier du simple espionnage à la déstabilisation d'un pays, en passant par le détournement des biens et des services, le vol ou la destruction d'informations, le harcèlement et le rançonnement, etc.

Les conséquences des cyber-attaques peuvent s'avérer désastreuses car la réussite des attaques cybernétiques peut fortement handicaper les commerces, les infrastructures critiques, les institutions ou organisations étatiques et autres, dans leurs opérations quotidiennes et provoquer des pertes importantes. Ces pertes, parfois très couteuses, peuvent conduire à des interruptions causées par l'indisponibilité des divers services informatiques. En somme, les désastres enregistrés peuvent être préjudiciables pour la souveraineté d'un pays, car «les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars.» disait Jean-Claude Juncker[1].

[1] Rapport d'information de la commission européenne sur le marché du numérique, E. Bothorel et Constance, LE GRIP, décembre 2017

Pour venir à bout du crime et de tout autre attaque en ligne, il est primordial de mener une lutte acharnée contre les malfaiteurs du cyberespace et les missions des «combattants numériques» incluent le durcissement des systèmes, la recherche, la veille et l'anticipation des menaces, l'audit, les tests d'intrusion, la supervision et la protection des systèmes d'information, la détection et la recherche des compromissions, l'investigation numérique et la veille sur les réseaux sociaux, la participation aux opérations.

Le Cameroun, à travers le Ministère des Postes et Télécommunications (MINPOSTEL), dans sa quête de sécurisation maximale de son cyberespace a procédé à un examen de ses capacités en matière de cybersécurité pour permettre à l'Etat de déterminer les domaines de capacité dans lesquels celui-ci pourrait investir de façon stratégique afin d'améliorer la cybersécurité et réduire la cybercriminalité. De ce rapport, il ressort que le Cameroun est assez avancé en ce qui concerne certains aspects de ses capacités. Aussi, il est opportun de les développer pour optimiser la gestion de la sécurité numérique. Il est aussi urgent d'engager des réflexions pour certains autres aspects pour lesquels les capacités sont au niveau embryonnaire.

Le développement des capacités est un processus de longue haleine, un moteur de changement et concerne l'individu comme premier agent de changement. Il concerne également la performance des organisations et l'environnement dans lequel baignent toutes les entités. A ce titre, il est souhaitable, voire impératif de développer, à la fois, le capital humain, la réalisation des infrastructures avec des équipements adaptés, ainsi que le contexte institutionnel et règlementaire qui doit être assaini ou bien établi. Cela permettrait de gagner en efficacité et en résilience. Cela permettrait également d'avoir un écosystème du numérique fonctionnel, performant et bien sécurisé.

La suite de cet article prévoit dans un premier temps, le rappel sur le cyberespace et ses défis dès l'origine. Ensuite, il est fait un état des lieux des capacités au Cameroun: puis, sont présentées les perspectives dans le développement des capacités. Et enfin, nous concluons.

I- LE CYBERESPACE ET SES DEFIS DEPUIS L'ORIGINE

Le cyberespace représente, à la fois, l'Internet et l'espace qu'il génère: un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance. Telle est, parmi les multiples définitions qui ont été énoncées dans diverses disciplines, par différents acteurs de différents pays, la définition empruntée[2].

Aussi, pour William Gibson, un romancier de science-fiction, inventeur du mot **cyberespace** dans son œuvre publiée en juillet 1982, *Burning Chrome* ou Gravé sur Chrome en français, le cyberespace désigne réseau informatique couvrant toute la planète, qui s'est installé au cœur de la vie quotidienne de la population. Le cyberespace est créé de nombreuses années après l'initiation de l'Internet dans les années 60 mais il se veut héritier de ses fonctionnalités qui se déclinent dans l'ambiance de la contre-culture des années 1960 et 1970 sur les campus californiens, un esprit d'ouverture, de liberté des échanges et de l'expression, d'autogestion qui touche au cœur même de l'architecture de l'Internet. Le réseau est pensé pour échapper au contrôle, décentralisé, pour que l'information puisse toujours contourner le blocage. Malheureusement, au fil des années, ce besoin de liberté de communication a donné naissance à une jungle numérique où règne une certaine anarchie parce que sans véritable autorité. C'est pourquoi, à partir du milieu des années 2000, le terme cyberespace réapparaît paradoxalement dans les discours des gouvernements, comme la représentation d'un territoire porteur de menaces, un territoire à contrôler, à surveiller, à conquérir, un territoire sur lequel il faut remettre des frontières et réaffirmer sa souveraineté. Un ensemble d'outils est, par conséquent, mis en place pour faire de cet espace un milieu sans danger. Des institutions sont créées pour assurer les missions organisationnelles, stratégiques et opérationnelles dans la préservation de la sécurité et en faire un espace où la lutte contre la mauvaise utilisation de l'Internet est assurée. Des textes juridiques et réglementaires sont également mis en place pour

[2] F. Douzet, Géopolitique du cyberespace: La cyberstratégie de l'Administration Obama, Geopolitics of cyberspace: the Obama administration's cyberstrategy, p. 138-149 https://doi.org/10.4000/bagf.1837

encadrer les dérives observées dans l'utilisation du cyberespace. Malgré ces efforts, d'assainissement du cyberespace, les attaques continuent de se propager dans le monde entier.

Au Cameroun, l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC), lors d'un récent atelier[3] organisé par le Ministère des Postes et Télécommunications (MINPOSTEL), présentait une cartographie des incidents répertoriés en 2021, donnant ainsi un aperçu des menaces auxquelles sont exposés les internautes camerounais ainsi que les Institutions. Cette cartographie (figure 1) se présente comme suit;

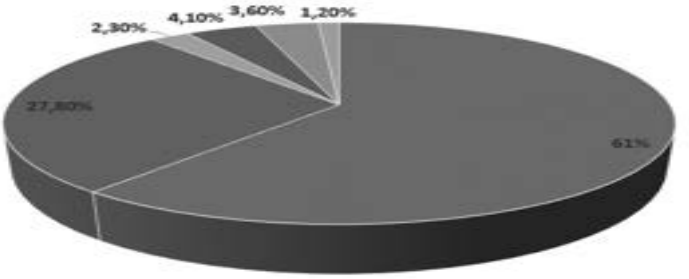


Figure 1: catographie d'incidents repertoriés en 2021 au Cameroun (source ANTIC)

L'ANTIC y présentait également une catégorisation des vulnérabilités du cyberespace au Cameroun. Trois catégories, physiques, organisationnelles et techniques sont répertoriées suivant les proportions suivantes de la figure 2;

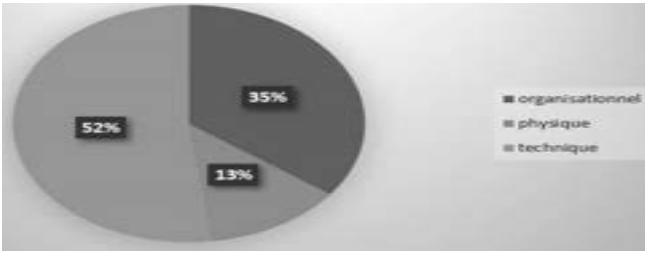


Figure 2:Catégorisation des vulnérabilités (source ANTIC)

Concernant les infrastructures critiques, après en avoir fait l'évaluation,

[3] Sensibiliser, traquer et sanctionner: l'ANTIC dans le dispositif stratégique des pouvoirs publics pour la promotion de la cybersécurité, P. Djousourbou Pagou

dans le secteur public et privé, l'ANTIC a révélé que le niveau de risque est très élevé au Cameroun;

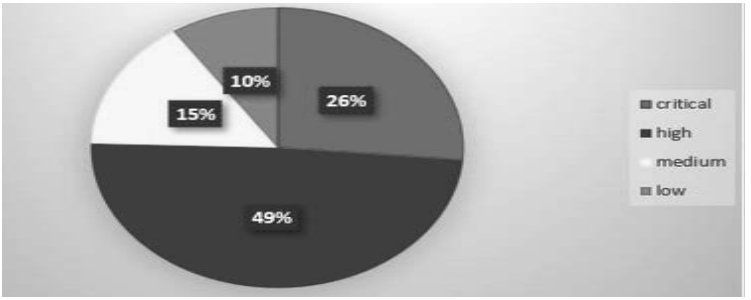


Figure 3: Niveau de risque des infrastructures (source ANTIC)

En définitive, au Cameroun comme partout dans le monde, le cyberespace est le terrain de diverses manœuvres malveillantes avec des desseins tout aussi divers. Ces manœuvres de cybermalveillance visent des objectifs politiques, économiques ou de sécurité et qui incluent des attaques contre des infrastructures critiques, du cyberespionnage et une surveillance de masse des citoyens. Le cyberespace est de ce fait à la fois un enjeu de rivalités, de pouvoirs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques (c). La prolifération des conflits entre une multitude d'acteurs exige donc de se pencher sur la problématique de renforcement des capacités de ces acteurs afin d'assainir les relations entre ceux-ci et d'assurer la pérennité de la démocratie, de la sécurité, de l'ordre public et même de l'autonomie du pays. Au préalable, ces capacités doivent être bien identifiées.

II- ETAT DES LIEUX DES CAPACITES EN CYBERSECURITE AU CAMEROUN

A- SITUATION GÉNÉRALE DES CAPACITÉS DE CYBERSÉCURITÉ AU CAMEROUN

Le Cameroun évalue régulièrement ses cybercapacités. Cela se fait souvent avec le concours de certains organismes internationaux qui ont mis

au point et utilisent des modèles pour la mesure du degré de maturité des pays et les niveaux de préparation de ces pays face aux cybermenaces. Plusieurs outils existent pour l'évaluation des capacités nationales en matière de cybersécurité, tels que l'indice mondial de Cybersecurité (GCI) de l'Union Internationale des Télécommunications ou encore, le modèle de maturité des Capacités en Matière de cybersecurité pour les Nations (CMN) du Centre Mondial de Capacités en Matière de Cybersécurité (GCSCC) de l'Université d'Oxford, et bien d'autres.

Dans le cadre de l'examen des capacités en matière de cybersécurité commandé par le Cameroun et exécuté par les experts de la Banque Mondiale (BM), il a été catégorisé quatre dimensions de capacités suivant le modèle de la BM: stratégies et politiques, culture de cybersécurité et société, éducation-formation-compétences, cadre juridique et réglementaire, normes-organisations et technologies.

S'agissant des stratégies et des politiques de sécurité, le Cameroun, par le MINPOSTEL, a élaboré en 2018, une politique nationale de sécurité des réseaux et des Systèmes de communication numérique qui comprend la Stratégie Nationale de cybersécurité. Ce document avait été rédigé en synergie avec plusieurs parties prenantes internes et internationales. Par ailleurs, la Stratégie Nationale de Développement[4] (SND30), au paragraphe 287 donne la vision sur le secteur de la cybersécurité ou de la sécurité du cyberespace.

Les capacités nationales du Cameroun dans la dimension «Cadres juridiques en matière de cybersécurité» sont assez avancées au vu de leur maturité. La loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et la cybercriminalité est le cadre juridique actuel régissant les questions liées au cyberespace au Cameroun[5]. Cette loi traite des TIC et comporte des dispositions plus spécifiques concernant la sécurité et l'intégrité des réseaux et services publics de communications électroniques. Elle régit également la protection de la vie privée et le traitement des données personnelles, l'utilisation abusive des ordinateurs et la cybercriminalité, la protection des enfants, la signature électronique et les transactions électroniques, entre autres. La loi N° 2010/012 du 21 décembre

[4] Stratégie Nationale de Développement 2020-2030 pour la transformation structurelle et le développement inclusif (SND30), 1re édition: 2020, ©Ministère de l'Économie, de la Planification et de l'Aménagement du Territoire

[5] https://www.minpostel.gov.cm/index.php/fr/les-textes/telecoms-tic/lois-telecoms-tic, consulté le 12 avril 2022

2010 relative à la cybersécurité et la cybercriminalité au Cameroun couvre également, mais pas spécifiquement, certains aspects concernant la protection de la vie privée, la liberté d'expression et les autres droits de l'homme en ligne (section IV).

La Constitution du Cameroun comporte de nombreuses dispositions ayant trait aux droits et libertés fondamentaux de l'homme, notamment la liberté d'expression, de conscience, de réunion, d'association et la liberté de circuler, le droit à la protection de la vie privée, les droits de l'enfant, entre autres, précisés dans le préambule et dans l'article 26[6]. Le code pénal est également un instrument important dans la mesure où il régit les actes qui portent atteinte à l'autorité de l'Etat, notamment, par la divulgation des documents administratifs; par les publications interdites à l'instar de celle d'un acte de procédure criminelle ou correctionnelle avant qu'il ne soit lu en audience publique: par violation de correspondance: ou encore par la violation du secret professionnel dans ses Articles 189, 300 et 310 respectivement[7].

Il existe également une loi sur le commerce électronique, la loi N° 2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun et une loi générale sur la propriété intellectuelle en adoptant la loi n° 2000/011 du 19 décembre 2000 relative au droit d'auteur et aux droits voisins, bien qu'elle ne soit aucunement une loi spécifique sur la propriété intellectuelle en ligne.

Au niveau international, le Cameroun n'a pas encore ratifié la Convention de Malabo. Celle de Budapest connaît une avancée favorable à sa ratification car le Président de la République du Cameroun a récemment promulgué, la loi N°2022/002 du 27 avril 2022, autorisant le Président de la République à procéder à l'adhésion du Cameroun à la Convention de Budapest sur la cybercriminalité. Il est à noter que ces deux conventions contiennent des chapitres sur les mécanismes de coopération et d'entraide internationale. D'autres mécanismes de coopération ont été instaurés avec d'autres pays comme le Tchad, la France et le Nigéria. Le Cameroun travaille également en étroite collaboration avec d'autres organisations, donc la Communauté Economique et Monétaire de l'Afrique

[6] Loi n°96/06 du 18 janvier 1996 portant révision de la constitution du 02 juin 1972, modifiée et complétée par la loi n°2008/001 du 14 avril 2008.

[7] Loi n°2016/007 du 12 juillet 2016 portant code pénal.

Centrale (CEMAC) et Interpol.

S'agissant des infrastructures, le Cameroun compte des laboratoires d'investigation scientifique relevant de la Police Nationale, de l'ANTIC, et du Secrétariat d'Etat à la Défense en charge de la Gendarmerie (SED). Le laboratoire de l'ANTIC est doté d'outils et d'équipements mis à jour, qui peuvent être utilisés pour extraire des données d'ordinateurs et de téléphones portables dans le cadre des enquêtes. Un système d'Infrastructure Nationale à Clé Publique (PKI) est en place à l'ANTIC pour favoriser l'utilisation de services d'administration électronique[8], et des outils évolués basés sur la cryptographie ont de ce fait été mis en place, dans certaines infrastructures et plateformes gouvernementales.

Dans le domaine de l'éducation et de la formation, le Gouvernement camerounais s'est donné comme vision de promouvoir le système éducatif et d'accroître l'offre de la formation professionnelle et technique de 10 à 25% au secondaire et de 18% à 35% au niveau supérieur. A cet effet, il est idoine d'intégrer le développement des capacités en matière de cybersécurité dès le plus bas niveau de l'éducation et d'aller crescendo jusqu'à atteindre, au niveau supérieur des offres de formation qui couvrent les pratiquement tous les aspects de cybersécurité. (SND30).

Le MINPOSTEL, tout comme les autres ministères utilisateurs des compétences en matière de sécurité numérique, dispose pour cela d'un plan de formation pour son propre personnel et fait un accompagnement vis à vis des autres structures étatiques et même des structures du secteur privé. Par ailleurs, un encadrement professionnel du Minpostel se fait à travers la mise en place ou le suivi des incubateurs. Dans ce sens, il a récemment été inauguré le Centre d'Innovation Numérique ou *Cameroon Digital Innovation Centre* (CDIC) qui est une infrastructure mise en place afin d'incuber et accompagner les jeunes entrepreneurs du numérique. L'organisation des compétitions et des concours est également un moyen d'émulation des compétences pour produire de l'innovation. Il y a également un accompagnement financier aux partenaires de la société civile et autres. Le Fonds des activités de Sécurité Electronique (FSE) créée avec la loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, a été mis en place pour assurer le

[8] https://web.antic.cm/, consulté le 12 avril 2022

financement de la recherche, du développement, de la formation et des études en matière de sécurité numérique. C'est ainsi que des financements sur les Fonds du Minpostel profitent aux personnels d'autres entités. Ce fonds a déjà eu à financer des projets tels que des laboratoires de cybersécurité à l'Ecole Nationale Supérieure Polytechnique de Yaoundé et d'autres laboratoires sont en vue dans les universités de Dschang, Maroua et Douala. Il a également eu à financer le laboratoire d'investigation numérique de la Délégation Générale à la Sureté Nationale (DGSN), entre autres équipements ou infrastructures de sécurisation numérique.

Dans le cadre de la culture de cybersécurité, le MINPOSTEL, l'ANTIC et bien d'autres entités étatiques ou du secteur privé s'attèlent à faire de la vulgarisation et de la sensibilisation auprès des citoyens à la bonne utilisation des TIC. De nombreuses campagnes de sensibilisation ont jusqu'ici été organisées, à l'instar de celle en cours pour la «sensibilisation à la cybersécurité et à l'usage responsable des réseaux sociaux». Des fora sont également organisés pour assurer le renforcement de la prise de conscience de la population sur la cybersécurité et offrir des cadres d'échanges et de partage d'expérience entre les acteurs du monde cybernétique.

B. ETAT DES LIEUX DE L'EXPERTISE CAMEROUNAISE EN MATIERE DE SECURITE NUMERIQUE

Pour pouvoir sauvegarder sa souveraineté dans le cyberespace global, le Cameroun se doit d'être autonome en matière de sécurisation de son écosystème numérique. Il est donc question de permettre à l'Etat du Cameroun de développer une expertise locale pour devenir complètement autonome sur les questions liées à la sécurité des réseaux et des systèmes d'information en général. Des avancées significatives sont faites dans ce sens car de nombreuses structures ou institutions étatiques et privées, sous la houlette de l'Etat camerounais, opèrent dans le secteur de la formation des camerounais en matière de sécurité numérique. Parmi ces institutions, nous avons les établissements universitaires suivants[9], notamment, le Centre de Recherche sur la Cyber sécurité et la Cyber défense de l'Université de Buea: L'École Nationale Supérieure des Postes et

[9] Etude sur la mise en place d'une PKI nationale par une expertise nationale - Livrable 1 réalisée par le cabinet ITS, 2019

Télécommunications et TIC (SUP'PTIC): Deux types de Master sont délivrés dans cette institution à savoir, le *Master of Engineering in Telecommunications* option Sécurité des Réseaux et Systèmes d'Information (SERES) et le Master Professionnel en Audit et Sécurité des Réseaux et Systèmes d'Information: Université de Maroua/l'Ecole Nationale Supérieure Polytechnique de Maroua avec son programme de masters spécialités Cryptographie et Sécurité Informatique (CRYP), Réseaux et Sécurité Informatique (RESE), Sécurité et Administration Réseaux (SAR) du Diplôme d'Ingénieur en Informatique: Université de Dschang avec son Master Professionnel en cybersecurité et gouvernance sécuritaire: l'Université inter-état d'Afrique Centrale de Sangmélima: l'Université de Yaoundé 1: l'École Nationale Supérieure Polytechnique-Agence Universitaire de la Francophonie: Master en Sécurité des Systèmes d'Information et de Communication (MASSICO): l'Université de Yaoundé I,: la Faculté des Sciences/ Département d'Informatique/ Recherches Doctorales dans le domaine de la cryptologie: l'Université Catholique d'Afrique Centrale avec son Master en Management et Systèmes d'Information: Etc.

De nombreux Camerounais reçoivent également ces enseignements dans les universités étrangères et reviennent mettre leur expertise au service de la sécurité numérique nationale. Cette expertise doit être développée de même que toutes les autres capacités évoquées plus haut.

III. LES PERSPECTIVES POUR L'AMELIORATION DES CAPACITES

Les cyberattaques se diversifient de plus en plus et sont en outre, sophistiqués et se multiplient rapidement; Ces attaques exigent d'accorder la priorité au renforcement des moyens de défense et au développement des cybercapacités pour parer à toute forme d'attaque. Certes, il y a des priorités et, nonobstant les moyens de financement, aucun aspect ne doit être mis de côté.

Pour assurer le renforcement des capacités, il est primordial de réviser et renforcer la stratégie de cybersécurité en place, fixer des objectifs réalistes, précis et ambitieux et définir de manière claire les mesures à

prendre, en faisant collaborer toutes les parties prenantes du cyberespace. Ce qui permettra de faire face aux défis persistants en matière de sécurité. En effet, l'existence d'une stratégie de cybersécurité est essentielle pour que la cybersécurité soit prise en compte dans tout l'appareil de l'État, car une stratégie contribue à faire de la cybersécurité un élément important de la politique publique, elle détermine les responsabilités et les missions des principaux acteurs gouvernementaux et non gouvernementaux en matière de cybersécurité, et elle affecte des ressources aux priorités et aux enjeux nouveaux et existants en matière de cybersécurité. Aussi, il est nécessaire de réviser la Stratégie Nationale de Cybersécurité en place ainsi que son plan d'action, afin de s'assurer que leur contenu tienne non seulement compte des composantes de référence, mais soit également en phase avec les besoins et priorités actuels du Cameroun dans le domaine de la cybersécurité et de la faire adopter. Dans cette stratégie, il faudrait mettre l'accent sur les compétences et les ressources locales car actuellement, le Cameroun importe des produits et des services de cybersécurité, ce qui augmente le risque de dépendance technologique et de vulnérabilité face aux opérateurs extérieurs mettant en danger le pays.

Il est sans doute fréquent qu'un incident se produise dans les systèmes d'information ou autres équipements du numérique par surprise et ce, malgré les efforts de sécurisation. À ce titre, nos capacités doivent nous permettre de toujours répondre énergiquement pour faire face aux attaques en cause. Aussi, est-il utile de préciser les fonctions du Centre de veille sécuritaire ou *Computer Incidence Response Team (CIRT)* en matière d'intervention en cas d'incident au niveau national et garantir une affectation suffisante des ressources technologiques, financières et humaines. Il faudrait également définir clairement la relation voulue entre le CIRT et les organismes privés compétents et s'assurer que celle-ci est comprise et efficace. Envisager d'inclure, dans le plan national de gestion des crises, les modalités d'intervention du pays en cas de crises liées à la cybersécurité et programmer l'organisation d'exercices de scénarios d'intervention d'urgence au niveau national avec la participation des parties prenantes concernées. Un centre de signalement des cyberdélits suffisamment équipé, devrait être créé et le public pourrait y signaler les cyberdélits et bien d'autres incidents, en appelant un numéro gratuit, en remplissant un formulaire en ligne ou en envoyant un courrier électronique.

Faire de ce centre un point d'entrée unique qui pourrait transférer des cas à d'autres parties prenantes[10].

Pour son cadre législatif et réglementaire, le Cameroun a besoin d'un cadre plus complet pour prendre en compte la cybercriminalité, et les questions y relatives, en particulier les procédures pour la sécurité des TIC et la gouvernance de la cybersécurité. Les cadres législatifs et réglementaires liés à la cybersécurité, sont relatifs à la vie privée, à la liberté d'expression et aux autres droits de l'homme en ligne, à la protection des données, à la protection des enfants, à la protection des consommateurs, à la propriété intellectuelle, ainsi que toutes les procédures en matière de cybercriminalité et autres.

Il est important de mettre en place un système de justice pénale. Celui-ci comporte la capacité des services de police et de justice à enquêter sur des cyberdélits, et la capacité du ministère public à présenter des dossiers pour des affaires de cybercriminalité ou faisant intervenir des preuves électroniques. Les magistrats doivent être capables de juger des affaires de cybercriminalité en faisant intervenir des preuves électroniques. Les enfants constituent l'une des couches les plus vulnérables et doivent particulièrement être protégés en tant que citoyens du futur. A cet effet, il y a lieu de compléter le cadre juridique en adoptant la loi sur la protection des enfants en ligne: Pareillement, il faut protéger les données personnelles de tous en adoptant la loi sur la protection des données personnelles, etc.

En matière d'éducation, le système éducatif doit être amélioré car il est important de proposer une offre d'enseignement de haute qualité en matière de cybersécurité avec un bon nombre d'enseignants qualifiés. Il y a également nécessité d'améliorer les enseignements par la professionnalisation et favoriser la collaboration entre les pouvoirs publics et l'industrie pour faire en sorte que les investissements dans ce domaine répondent aux besoins de l'environnement de cybersécurité.

Le développement continu des compétences exige l'existence et la fourniture de programmes de formation en cybersécurité permettant de constituer un corps de professionnels de la cybersécurité permettant le transfert horizontal et vertical des connaissances en cybersécurité à l'intérieur des organisations. Il y a lieu de noter que les cours

[10] Rapport sur l'Examen des Capacités En Matière De Cybersécurité au Cameroun réalisé par la Banque Mondiale, 2019

d'informatique sont dispensés dans toutes les universités du Cameroun. Mais, ces cours ont été modifiés pour y inclure des composantes de cybersécurité. Aussi, faudrait-il prévoir un programme de qualification ciblant les enseignants en cybersécurité. En outre, un système d'agrément pour l'enseignement de la cybersécurité doit être mis en œuvre. Egalement, pour que les étudiants puissent mettre en pratique les apprentissages théoriques, des ressources et des outils devraient être suffisamment mis à leur disposition. Il est question ici de mettre en place un plan de formation d'experts sur le terrain, notamment via des certifications internationales. De toutes les manières, il est urgent d'améliorer l'enseignement de la cybersécurité dans les écoles d'ingénieurs et les universités. L'une des pistes à la réalisation de cette ambition étant la mise en place d'un forum de collaboration continue entre le monde universitaire, le secteur privé et le secteur public, afin de fournir les ressources nécessaires pour l'enseignement de la cybersécurité.

Malgré la mise en place des incubateurs numériques, l'organisation annuelle de la semaine du concours de l'innovation numérique et l'organisation des camps TIC, il y a nécessité de proposer des bourses pour permettre aux étudiants de poursuivre des études universitaires de deuxième et troisième cycle dans les TIC. L'on pourrait également élaborer et institutionnaliser des programmes de formations spécialisées pour les agents des services de Police et de Justice, notamment les Policiers, les Procureurs et les Juges, sur la cybercriminalité, les preuves électroniques et la protection des données à caractère personnel. Ce qui améliorerait leurs prestations sur le terrain.

L'intégration de technologies innovante et connexe dans les filières de formation en sécurité numérique doit être effective. Par exemple, avec l'intelligence artificielle, les technologies prédictives basées sur le goût ou les habitudes et désirs des utilisateurs de l'Internet permettent aujourd'hui de mieux sécuriser par la surveillance des individus qui pourraient être considérés à risque puisqu'ils sont de potentiels criminels. L'intégration de l'Intelligence Artificielle (IA) dans les cybercapacités physiques, notamment au niveau des liaisons de communication et de données entre les véhicules ou tout autre équipement terminal, peut entraîner des vulnérabilités aux attaques de guerre électronique telles que le brouillage, l'usurpation ou le piratage; Une action contraire bénéfique peut également être menée.

Tout ceci mis en œuvre doit être vulgarisé suffisamment et tout le monde, utilisateurs, professionnels de sécurité, doivent être suffisamment sensibilisés car donner la bonne information lutterait mieux contre moult fléaux de société à l'instar de la désinformation, la propagande, etc.

CONCLUSION

Ayant pris conscience des enjeux qu'impose la recrudescence des actes de cybercriminalité dans le cyberspace global, et camerounais en particulier, il est question de coordonner et de redoubler d'efforts pour mettre à disposition des capacités efficaces tout en inculquant aux citoyens une solide culture en matière de cybersécurité pour un pays sécurisé et paré à toute épreuve en matière d'attaques cybernétiques. Au Cameroun, il existe des capacités avec des degrés de maturité divers, pas suffisamment élevés pour certaines et basiques pour d'autres. Il y a de ce fait, des améliorations à fournir pour avoir des stratégies et politiques qui fixent des objectifs réalistes, précis et ambitieux et définissent de manière claire les mesures à prendre pour une meilleure sécurisation du cyberespace: le cadre juridique et réglementaire doit être révisé pour mieux encadrer et mieux réguler le domaine de la sécurité numérique: l'ensemble éducation-formation-compétences doit être réformé pour permettre d'avoir un bon nombre de professionnels de la cybersecurité et disposer d'une expertise locale avérée.

Il ne faut surtout pas perdre de vue que le maillon le plus faible de la chaine sécurité est la ressource humaine, la capacité humaine. Sans négliger les autres capacités, un accent devrait être mis sur le renforcement des capacités humaines de tous les acteurs impliqués, en tant qu'élément pensant et manipulant les autres capacités, à travers divers types de formations de base ou continues ainsi que l'éducation des masses par des campagnes de sensibilisation et l'organisation des fora, pour assurer le renforcement de la prise de conscience de la population et de toutes les parties prenantes sur la cybersécurité et sur tous les types de cyberattaques.

BIBLIOGRAPHIE

1 https://www.minpostel.gov.cm/index.php/fr/les-textes/telecoms-tic/lois-telecoms-tic, consulté le 12 avril 2022

2 https://web.antic.cm/, consulté le 12 avril 2022

3 Loi N°2016/007 du 12 juillet 2016 portant code pénal

4 Loi N°96/06 du 18 janvier 1996 portant révision de la constitution du 02 juin 1972, modifiée et complétée par la loi n°2008/001 du 14 avril 2008

5 Stratégie Nationale De Développement 2020-2030 pour la transformation structurelle et le développement inclusif (SND 30), 1re édition: 2020, ©Ministère de l'Économie, de la Planification et de l'Aménagement du Territoire

6 Rapport d'information de la commission européenne sur le marché du numérique, Eric Bothorel et Constance LE GRIP, décembre 20173

7 Etude sur la mise en place d'une PKI nationale par une expertise nationale - Livrable 1 réalisée par le cabinet ITS, 2019

8 Rapport sur l'Examen des Capacités En Matière De Cybersécurité au Cameroun réalisé par la Banque Mondiale, 2019

9 Géopolitique du cyberespace: La cyberstratégie de l'administration Obama, Geopolitics of cyberspace: the Obama administration's cyberstrategy, Frédérick Douzet, p. 138-149 https://doi.org/10.4000/bagf.1837

10 Sensibiliser, traquer et sanctionner: l'ANTIC dans le dispositif stratégique des pouvoirs publics pour la promotion de la cybersécurité, P. Djoursoubou Pagou

QUELLES APPROCHES FACE AU DEVELOPPEMENT DES MENACES MEDIACRATIQUES ?

Justine DIFFO TCHUNKAM
Professeur Titulaire des Universités - Cameroun
Présidente du Conseil d'Administration de l'Agence de Régulation des Télécommunications

RESUME

La réalité de la démocratisation des médias cybernétiques charrie beaucoup d'enthousiasme chez les jeunes et chez bien d'autres usagers férus du sensationnel à travers les médias sociaux. La révolution numérique en marche, au-delà des nombreux enjeux économiques et sociaux qu'elle draine, recèle également des défis importants, eu égard aux nouvelles menaces qui en émergent au fil du temps et des découvertes. La présente contribution, au demeurant, regroupe ces diverses menaces sous le vocable de «*menaces médiacratiques*», en questionnant les approches susceptibles d'y répondre efficacement. Ainsi, à la question de savoir comment faire face aux nouvelles menaces contemporaines émergeant de la démocratisation de l'usage des TIC, l'impératif d'une démarche concertée s'impose, donnant prime à une conception uniforme des menaces médiacratiques et à la recherche de coordination dans la réponse cybersécuritaire y relative.

MOTS CLÉS;

Menace médiacratique – Cybercriminalité – Cybersécurité – Numérique – Cyber-attaque.

INTRODUCTION

Dans un environnement où la démocratisation de l'usage des technologies de l'information de la communication aidant, la révolution numérique s'accélère, bouleversant au passage nos modes de vie et de pensée[1] au point de se muer en une véritable culture[2] ayant ses enjeux propres[3], il semble opportun de scruter l'horizon tracé par le numérique. Perçu comme la nouvelle révolution industrielle, le phénomène constitue la transformation la plus radicale que connaissent les nations depuis la révolution industrielle[4]. Peu à peu, les technologies numériques s'incrustent dans nos vies pour constituer une véritable *culture du numérique*[5]et tel *Janus*, elles rassurent tout autant qu'elles inquiètent.

De plus en plus présent dans notre vocabulaire, le vocable «*numérique*» est devenu «*un mot passe-partout qui sert à définir un ensemble de pratiques qui caractérise notre quotidien et donc nous avons peut-être encore du mal à saisir la spécificité*»[6]. Son usage récurrent emprunte aux termes évocateurs tels que: *gouvernance numérique*, *économie numérique*, *identité numérique*, *smart contract*, *e-management*, *Fintech, Finance digitale, e.insurance, cryptomonnaie*, *bitcoin*, etc., désormais très courants, et qui ne manquent pas d'entretenir l'épineux problème d'insécurité juridique dû à la quasi-absence ou aux difficultés de réglementation efficace de certaines réponses technologiques portées par la créativité et l'ingéniosité humaine face aux défis sociaux. Il en va ainsi de l'occurrence quasi-spontanée de comportements criminels multiformes qui se développent au quotidien, et que l'on pourrait regrouper

---

[1] Brunet F., Le numérique, levier d'une croissance, Rapport de la Commission Economie et Croissance, adopté en Assemblée Générale le 19 décembre 2013, CCI, Paris-Ile-de-France, p.4.

[2] Vitali -Rosati M., «*Pour une définition du numérique*», In *Pratique de l'édition numérique* (sous la direction de M. Vitali –Rosati et M. E. Sinatra, Presses universitaires de Montréal, Montréal, 2014, Chapitre 4, pp.63-75.

[3] M. Vitali –Rosati, «*Pour une définition du numérique*», In *Pratique de l'édition numérique* (sous la direction de M. Vitali-Rosati et M. E. Sinatra , Presses universitaires de Montréal, Montréal, 2014, Chapitre 4, p.69.

[4] Voir rapport du Ministère du revenu national sur «*Le commerce électronique et l'administration fiscale du Canada*», présenté par le Comité consultatif ministériel du commerce électronique, avril 1998: cité par

H. Lachaize, *La notion d'établissement stable à l'épreuve du commerce électronique*, Mémoire de D.E.A, Faculté des Sciences Juridiques et Politiques, Université R. Schuman– Strasbourg, 1999. D'ailleurs, l'économiste américain J. Rifkin, voit en l'émergence de l'économie numérique une *3e révolution industrielle*: propos rapporté par N. Guiland, *La TVA et les services électroniques: l'appréhension de l'immatériel par la fiscalité indirecte*, Rapport de recherche, Master I droit des affaires, Faculté de droit et science politique, Université d'Aix-en-Provence, 2014-2015, p.9.

[5] M. Vitali –Rosati, «*Pour une définition du numérique*», In Pratique de l'édition numérique (sous la direction de M. Vitali –Rosati et M. E. Sinatra, Presses Universitaires de Montréal, Montréal, 2014, Chapitre 4. [6] Idem, p.64.

sous la terminologie générique de *menaces médiacratiques,* bien connues dans le champ matériel de la *cybercriminalité*. Il s'agit de l'«ensemble des infractions s'effectuant à travers le cyberspace par d'autres moyens que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique»[6].

En effet, la dynamique mondiale irréversible vers la société digitale favorise la numérisation de notre quotidien, et ouvre désormais comme une voie royale aux cybercriminels qui se saisissent les failles et des dysfonctionnements des systèmes numériques parfois en pleine construction voire en cours d'évaluation, pour commettre leurs forfaits. D'ailleurs, leurs outils s'en trouvent de plus en plus sophistiqués, faisant émerger de nouveaux phénomènes à l'instar de «*cybersquatting*», «*hacking*», «*phishing*» ou fraude à l'identité numérique. Menace sans frontière, polymorphe et en pleine expansion, la cybercriminalité qui aujourd'hui retient l'attention de l'ensemble des systèmes juridiques au monde, à en croire C. Morin, est incontestablement une des plus importantes menaces de ce 21e siècle[8]. Face à l'immatérialité, l'internationalité et la volatilité, facteurs de la grande complexité qui caractérise ces nouvelles formes de la criminalité, ouvrir une réflexion sur les voies à explorer dans le cadre de la recherche de solutions efficaces contre les menaces médiacratiques s'avère opportune. Il s'agit, plus concrètement, de répondre à la question de savoir comment faire face aux nouvelles menaces engendrées et paradoxalement soutenues par la démocratisation de l'usage des technologies du numérique.

Cette problématique est d'autant plus intéressante qu'elle interpelle sur les craintes qu'entrainent aujourd'hui la démocratisation des TIC, en termes de régulation attendue, notamment quand l'on envisage les lignes d'insécurité qui en émergent. D'ailleurs, en référence à une certaine doctrine[7], face à la déferlante de l'intelligence cybercriminelle actuelle, il y a lieu de réagir rapidement pour mettre en place une fonction d'*intelligence juridique* capable d'anticiper afin de pallier les revers de l'évolution exponentielle des technologies par le support des média sociaux. Dans ce sens, J.-L. Bergel soutient à juste titre que «*le droit ne cesse d'évoluer dans un monde qui change*

[6] - Article 4-32 de la Loi N°2010/012 du 21 décembre 2010 sur la cybersécurité et la cybercriminalité au Cameroun. [8] Morin C., «*La criminalité investit le cyberespace*», Dossier Gendinfo, mise en ligne le 21 janvier 2019. Disponible sur: *www.gendinfo.fr*

[7] G. Guglielmi, «Présentation du huitième numéro sur les nouvelles technologies et le droit», Jurisdoctoria, n°8, 2012, p.12. Disponible sur: *https://www.jurisdoctoria.net*. Selon l'auteur,

(…): les juristes travaillent (…) pour traiter des réalités de la vie et des relations humaines (…) qui ne cessent de se développer et de se transformer»[8]. Ne pouvant donc pas se résoudre à ce que l'on connait fort bien en droit positif et qui risque de ne pas suffire pour répondre aux nouvelles situations et aux nouveaux besoins, il importe naturellement de proposer, voire «*d'inventer d'autres instruments et d'autres méthodes, d'imaginer des solutions nouvelles, d'anticiper sur un droit en perpétuel devenir*»[11]. Dans cette optique, et parce qu'il faut, avant toute tentative de solution, cerner clairement l'ampleur de la menace cybercriminelle actuelle, C. Juiff indique que si la cybercriminalité était mesurée comme une économie, elle caracolerait en troisième place du classement mondial derrière les Etats-Unis et la Chine. Il en va ainsi compte tenu des 6000 milliards de dollars US de dommages infligés au monde en fin 2021 par le phénomène cybercriminel.

Ainsi, répondant à la question au cœur de cette réflexion, une lecture du cadre législatif confrontée aux modes opératoires des menaces médiacratiques permettrait d'observer que la lutte contre la nouvelle donne criminelle appelle une approche concertée tant dans sa compréhension que dans la réponse sécuritaire y afférente. Autrement dit, contrer ces menaces contemporaines découlant de l'usage des technologies numériques impose une approche globale souhaitée et unifiée de la conception des menaces médiacratiques (I) d'une part, et une coordination recommandée de la réponse cybersécuritaire y relative, d'autre part (II).

I. UNE APPROCHE GLOBALE SOUHAITEE ET UNIFIEE DES MENACES MEDIACRATIQUES.

C'est une lapalissade que la protection de l'espace cybernétique ou cyberespace est aujourd'hui une question majeure[14] dont la compréhension passe par une appréhension uniforme des menaces susceptibles d'en émerger. En effet, il convient à bien des égards, de mettre en exergue une constance, à savoir qu'à l'ère du numérique, les tendances subissent des transformations,

[8] J-L. Bergel, «*A la recherche des concepts émergents en droit*», Recueil Dalloz, 2012, p.1567: voir dans le même sens, Le Cannu P. (dir), *D'un côté à l'autre: le droit commercial en mouvement*, LGDJ, 2008: P. Bloch et S. Schiller (dir), *Quel code de commerce pour demain ?*, Lexis-Nexis, 2007: Cour de cassation et

Cela dit-il, il importe, compte tenu de la présomption d'internationalité des nouvelles menaces opérant via les technologies du numérique, en l'occurrence l'internet, de favoriser une certaine unicité de compréhension de ces menaces en en élucidant le sens et les enjeux. La régulation des Fakes News et avis factices sur les plateformes postulerait alors et sans doute une clarification avisée du concept de menace médiacratique (A), avant de présenter les visages de la criminalité cybernétique (B).

A. L'INTELLIGIBILITÉ DU CONCEPT DE MENACE MÉDIACRATIQUE OU CYBERDÉLINQUANCE

Les menaces médiacratiques, appréhendées de préférence par les juristes sous le vocable générique de cyberdélinquance ou cybercriminalité, au-delà de l'absence de définition conventionnelle ou même légale, peuvent se concevoir comme toutes actions ou activités illégales dont l'objet est de perpétrer des infractions pénales sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunications[9]. Quoique non définie, la cybercriminalité présente, toutefois, plusieurs caractéristiques: il s'agit d'une criminalité organisée, mondialisée et transnationale par nature[17]. Non seulement, les frontières n'arrêtent pas les cyberdélinquants, mais elles leur permettent d'échapper aux poursuites[10]. L'on peut lire dans les travaux d'INTERPOL[11] que les organisations criminelles privilégient de plus en plus Internet pour faciliter leurs activités et réaliser des bénéfices maximum en un minimum de temps. La criminalité de très haute technologie comme le piratage informatique, les attaques par logiciel malveillant, et l'extorsion DDoS[12], représente une menace réelle pour la sécurité des gouvernements, des entreprises, et des particuliers. Elle présente, en outre, d'importants défis pour les services chargés de l'application de la loi, car de nombreux pays ne disposent pas encore de la connaissance ou des compétences techniques nécessaires pour y faire face.

[9] S. Joissains et J. Bigot, Rapport d'information (sur la lutte contre la cybercriminalité), Sénat, N°613, 09 Juillet 2020, Session extraordinaire de 2019-2020, p.6. [17] S. Joissans et J. Bigot, Rapport d'information (sur la lutte contre la cybercriminalité), Sénat, N°613, 09 juillet 2020, Session extraordinaire de 2019-2020, p.6.

[10] Idem.

[11] Interpol Foundation, Cybercriminalité, Cyberbrochure, février 2017, 12 pages. Consultable sur; *www.interpol.int*

[12] Distributed Denial of Service ou déni de service distribué

L'utilisation accrue de la technologie, l'internet en l'occurrence, pour commettre les infractions comme les vols, la fraude, et même le terrorisme qui ajoute une nouvelle dimension à ces activités criminelles «*traditionnelles*»[13].

B. LES VISAGES DE LA CYBERDELINQUANCE OU CYBERCRIMINALITE

Selon M. Quemener [22], l'internet, compris comme «*un outil pour l'acte et transgression*» offrant une potentialité importante de fraude[14], constitue un vecteur de développement d'infractions. En effet, indique l'Avocat Général près la Cour d'Appel de Versailles, «*on est passé d'une délinquance classique à une délinquance numérique, causant des préjudices qui ne sont pas virtuels et qui ne cessent d'augmenter*»[15]. D'ailleurs, peut-on le constater, la criminalité, et en particulier la criminalité économique et financière, prend désormais une connotation «*cyber*» comme toutes les activités illicites avec le développement de l'internet et des réseaux numériques. La croissance observable de la connectivité est à l'origine de la montée en puissance de la criminalité informatique qui, convient-il de le rappeler, constitue l'une des dix formes recensées de criminalité grave ayant une dimension transfrontière. Tel Janus, le numérique propose sa face la plus sombre en offrant des opportunités nouvelles pour les délinquants cybernétiques[16].

La dématérialisation des flux de transactions aidant, l'accroissement de l'anonymat et la déportation des lieux de commission des infractions dans le cyberespace, semble-t-il, facilite le passage à l'acte des délinquants. Ainsi, entre cyberfraudes, escroqueries, faux ordres de virement, cyberarnaque et autres piratages de données à caractère personnel constituant l'apanage de ce qu'il est convenu de nommer «*Darknet*», le droit pénal de fond et de forme est rudement mis à l'épreuve. Aussi, convient-il d'observer que la cybercriminalité ou cyberdélinquance vise;

---

[13] Idem, p.5. [22] Avocat Général près la Cour d'Appel de Versailles.

[14] Propos d'E. Chirat in Cyber cercle, «*Criminalité économique et financière à l'heure du numérique*», mis en ligne le 25 février 2015. Disponible sur: *www.cybercercle.com*

[15] In Cyber cercle, «*Criminalité économique et financière à l'heure du numérique*», mis en ligne le 25 février 2015. Disponible sur: *www.cybercercle.com*

[16] Voir dans ce sens, M.Quemener, «*Cybercriminalité: la délinquance économique du 21e siècle*», In Sécurité et Défense Magazine, 18 juillet 2015. Disponible sur: *www.SD-magazine.com*

- soit des **infractions spécifiques à Internet**, pour lesquelles les technologies de l'information et de la communication sont l'objet même du délit, par exemple les atteintes aux systèmes de traitements automatisés des données, les infractions en matière de fichiers ou de traitement informatique ou encore le domaine de la cryptologie: il s'agit d'infractions nouvelles spécifiques à Internet, relevant du piratage informatique, c'est-à-dire l'intrusion non autorisée dans les systèmes informatiques et le sabotage informatique de ceux-ci;
- soit des **infractions de droit commun dont Internet permet la commission**: il s'agit, dans ce cas, de formes traditionnelles de criminalité ou d'infractions de droit commun préexistant à Internet, mais qui se sont développées grâce à lui. Ce sont, entre autres, la propagation de fausses nouvelles[17], l'abus de confiance, l'escroquerie, la violation de correspondance, les délits d'opinion, les atteintes diverses aux mœurs à l'instar de la pédopornographie.

II. UNE COORDINATION RECOMMANDEE DE LA REPONSE CYBERSECURITAIRE

Au-delà de l'uniformité recherchée dans la compréhension du concept de menace médiacratique, une réponse cybersécuritaire, pour le moins, coordonnée constitue le gage de sécurisation de l'espace cybernétique. L'idée de fond ici consiste, en prenant la pleine mesure des défis à surmonter face à ces menaces, de suggérer une mutualisation des efforts des gouvernements dans la riposte contre le nouveau phénomène cybercriminel. Ainsi, avons-nous pensé qu'une riposte efficace contre les risques d'attaques cybernétiques impose de constater la nécessité de structuration au niveau national ou local de la réponse cybersécuritaire d'une part (A), et l'opportunité d'une riposte organisée au niveau international face aux menaces médiacratiques d'autre part (B).

[17] Lire dans ce sens, E.Marique et A. Strowel, «*La régulation des Fakes News et avis factices sur les plateformes*», Ride, De Boeck Supérieur, 2019, Tome XXXIII, pp.383-398. Consultable sur: *http://www.cairn.info/revue-internationale-de-droit-economique-2019-3-page-383.htm*;

A. LA NECESSITE DE STRUCTURATION DE LA REPONSE CYBERSECURITAIRE NATIONALE

Face à la résurgence observable des menaces médiacratiques, il importe pour chaque gouvernement territorial dans le cadre de la réponse cybersécuritaire nationale de garantir une certaine structuration. Car, en effet, l'intelligence qui pilote ces vagues de comportements, faudrait-il le rappeler, impose de développer en face une intelligence juridique et technologique à la fois proactive, active et réactive: capable, dans une certaine mesure, d'en venir à bout. Aussi importe-t-il dans le contexte actuel de constater que l'humain demeure, en tout état de cause au centre de la lutte contre les cybermenaces[18]. Ainsi, pensons-nous, à ce niveau, qu'une réponse efficace face à ce nouveau phénomène criminel réside dans la trilogie: *recherche*, *éducation* et *dialogue* avec les acteurs. Le potentiel de la recherche en matière de lutte contre la cybercriminalité grandissante suggère de mettre en place un *Bureau National d'Intelligence Cybernétique* (BNIC) au sein duquel seraient représentés les forces de sécurité, l'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC), la communauté universitaire et autres spécialistes de la cybersécurité. En clair, il s'agirait d'une sorte de *Cyber Threat Intelligency Lab*, véritable organisme de veille cybersécuritaire dont la vocation serait de créer un socle commun de connaissances sur les menaces cybernétiques, en contribuant au développement des solutions dans la lutte contre les cybermenaces.

Le volet éducation quant à lui, est le lieu, en recentrant la position de l'humain dans la lutte contre les risques de cyber-attaques, d'assurer;

une certaine éducation à l'usage des technologies à travers sensibilisation à un usage citoyen des TIC et aux risques divers de cyber-attaques;

une sensibilisation des institutions et autres organisations sur la nécessité de disposer des systèmes d'alerte en cas de cyber-attaque[19], et surtout de

[18] Voir dans ce sens, JUIFF (C), «*Faire face ensemble: plaidoyer pour le développement d'une approche collective face aux risques cyber*», Op. cit. Disponible sur: *https://alcyconie.com/faire-face-ensemble-plaidoyerpour-le-developpement-dune-approche-collective-face-aux-risques-cyber/*

[19] Idem.

partager les renseignements et les informations des éventuelles cyber-attaques dont ils seraient l'objet[20].

S'agissant *in fine* du dialogue des acteurs, il ressort du propos de Léon Juste IBOMBO[21] que le développement du partenariat public-privé constitue un sérieux gage de mise en place d'organes d'alerte et de lutte contre les cybermenaces d'une part, et de financement des investissements dans le secteur du numérique d'autre part[22].

B. L'OPPORTUNITE D'UNE RIPOSTE INTERNATIONALE ORGANISEE FACE AUX MENACES MEDIACRATIQUES

Faire face aux risques médiacratiques impose absolument l'organisation d'une réponse collective. D'ailleurs, l'internationalité ou même la mondialité des risques de cyber-attaques somme toute inhérentes aux technologies numériques, ne fait plus de doute dans un contexte marqué par l'extrême vulnérabilité des organisations à la nouvelle criminalité. Dans ce sens, C. Juiff n'indique-t-elle pas que «*galvaniser leurs profits, les sponsorships étatiques et les nombreuses opportunités développées par la digitalisation rapide mais insuffisamment sécurisée des organisations, les structures cybercriminelles sont (…) devenues des multinationales du crime par leur taille et leur fonctionnement*»[23]. D'ailleurs, observe-t-on face à cette recrudescence de vents incultes et dans un élan de construction de ce qu'il est convenu de nommer *cyberdroit*[24], une réaction des législations internationales, régionales[25] ou

[20] Cela est d'autant plus important que C. Juiff indique dans ses travaux la tendance pour les organisations, souci de préserver leur notoriété, à ne pas communiquer sur les attaques cybercriminelles dont ils sont souvent l'objet. Toute chose qui ne facilite pas la prévention de telles attaques auprès d'autres organisations ou en cas de récidive (Voir JUIFF (C), «*Faire face ensemble: plaidoyer pour le développement d'une approche collective face aux risques cyber*», Op. cit. Disponible sur: *https://alcyconie.com/faire-face-ensemble-plaidoyer-pour-ledeveloppement-dune-approche-collective-face-aux-risques-cyber/*).

[21] Ministre des postes, télécommunications et de l'économie numérique en République du Congo.

[22] Propos du Ministre des postes, télécommunications et de l'économie numérique en République du Congo, Léon Juste IBOMBO, au micro de Cio Mag, recueilli par Souleyman Tobias, 29 mars 2022. Disponible sur: *https://cio-mag.com/cybersecurite-nous-avons-un-instrument-pertinent-qui-malheureusement-nest-pas-encoreapplicable-leon-juste-ibombo/*

[23] Lire dans ce sens et avec un certain intérêt, l'article de C. Juiff , «*Faire face ensemble: plaidoyer pour le développement d'une approche collective face aux risques cyber*», Op. cit. Disponible sur: *https://alcyconie.com/faire-face-ensemble-plaidoyer-pour-le-developpement-dune-approche-collective-face-auxrisques-cyber/*

[24] Lire avec beaucoup d'intérêt, Feral –Schuhl (Chr.), *Cyberdroit. Le droit à l'épreuve de l'internet*, Paris, Dalloz, 4e éd., 2006: N'TCHATAT TOUNYA (F-L), Le cyberdroit dans l'espace OHADA, mémoire de master 2, Université de Yaoundé

communautaires[26] et même nationales[36] tendant à l'adaptation du droit actuel à la *cybermondialisation* du crime.

Les cybermalfaiteurs n'ayant de cesse de faire évoluer leurs modes opératoires, INTERPOL suggère une adaptation de la riposte cybersécuritaire à travers;

- la mise en place d'une **plateforme d'information et d'analyse**. A l'effet de répondre aux nouveaux enjeux de la lutte contre la cybercriminalité, les services chargés de l'application de la loi doivent adopter une nouvelle approche en matière d'échanges d'informations de police, capables de soutenir le rythme rapide des développements des enquêtes sur la cybercriminalité et de l'informatique légale.
- la mise en place d'un **dispositif d'évaluation des cybermenaces**. INTERPOL mène un travail constant pour élaborer de nouvelles méthodes afin que les pays membres soient sensibilisés aux cybermenaces les plus récentes, et qu'ils acquièrent les outils nécessaires pour les combattre. Aussi, sont-ils encouragés à publier les notices et diffusions INTERPOL pour alerter toutes les polices du monde sur les menaces connues. Des recherches vont être menées pour établir une prospective stratégique sur les tendances de la cybercriminalité, par exemple la vente par les malfaiteurs de leurs outils de cybercriminalité au soumissionnaire le plus offrant dans le cadre d'une «*prestation de criminalité*», ce qui aidera les pays membres à mieux se préparer au plan opérationnel. En parallèle, INTERPOL travaille au développement d'outils pour lutter contre ces menaces.
- la **mise en relation des mondes numériques et physiques**. Les «indices» électroniques susceptibles d'identifier les auteurs d'actes de cybercriminalité sont souvent détenus par des entités privées comme les fournisseurs d'accès à Internet, qui disposent d'équipes spécialisées

II, 2014.

[25] La convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, du 27 juin 2014, Malabo (Guinée Equatoriale).

[26] Les projets de lois types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et de directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) relatif à la protection des données à caractère personnel: aux transactions électroniques et à la lutte contre la cybercriminalité. [36] Loi n°2010/012 du 21 déc. 2010 sur la cybersécurité et la cybercriminalité au Cameroun.

pour gérer les incidents de sécurité. INTERPOL va s'engager dans un effort de sensibilisation dans le but de former la communauté privée de la sécurité aux exigences des enquêtes dans le cyberespace et d'établir des relations constructives afin que les enquêteurs des services chargés de l'application de la loi puissent avoir accès aux renseignements détenus par le secteur privé. La capacité à mettre en corrélation les informations numériques (adresses IP, identifiants des périphériques mobiles) et les informations physiques (données biométriques, localisations) afin d'identifier les suspects d'actes de cybercriminalité va constituer un nouveau domaine d'intervention de la plus haute importance. De ce fait, INTERPOL va identifier et tester les méthodes et les technologies d'enquête récentes les plus prometteuses en collaboration avec le secteur privé et le monde universitaire. Elles peuvent porter sur la reconnaissance faciale, la reconnaissance d'objets sur la base d'images, l'analyse de textes et l'analyse intégrée pour lier la cybercriminalité et les cybercriminels au monde physique.

CONCLUSION

A la question de savoir comment faire face aux menaces contemporaines émergeant de la démocratisation de l'usage des technologies du numérique, il est donné d'affirmer avec C. Juiff[27] que face à ce vent de menaces globales, l'organisation d'une riposte collective et coordonnée est d'une nécessité absolue. En effet, il s'avère qu'en règle générale, répondre efficacement aux menaces médiacratiques impose une démarche concertée aussi bien dans la compréhension du phénomène que dans la riposte cybersécuritaire y afférente. Cette démarche empruntée à la méthodologie scientifique des politiques criminelles s'applique aisément à la présente problématique, en postulant une conception uniforme des menaces médiacratiques dans le contexte planétaire spécifique dominé par le phénomène de la criminalité dans le cyberespace: en contextualisant ce phénomène dans le cyber environnement médiatique

[27] C. Juiff, «*Faire face ensemble: plaidoyer pour le développement d'une approche collective face aux risques cyber*», Op. cit. Disponible sur: *https://alcyconie.com/faire-face-ensemble-plaidoyer-pour-le-developpementdune-approche-collective-face-aux-risques-cyber/*

dominant, l'on appréhende aisément l'impact des dynamiques numériques en cours, à l'aune de la double influence de *mutation* et d'*amplification* caractérisant les technologies numériques en support.

Quant à l'idée de riposte cybersécuritaire coordonnée face aux menaces médiacratiques, il est clair que son efficacité est largement tributaire de la structuration ou de l'organisation au double plan national et international de la réponse sécuritaire face à ces menaces. Toute chose qui semble à la portée du législateur, lorsque l'on sait que «*pour les juristes, le cyberespace bouge, trépigne et chahute avec d'autant plus de vigueur que ces derniers ont justement pour fonction de contrôler l'évolution du monde qui les entoure*»[28], étant entendu que «*le droit est en effet une science de la réaction dont l'une des missions premières est de savoir ce que sera demain*»[29].

Aussi, émerge-t-il de cette réflexion des pistes de solutions envisageables, si tant est que la fonction sociale du juriste est celle «*d'aider à la solution des conflits et des doutes juridiques, celle de contribuer à déterminer la voie à suivre*»[30]. Il s'agit, entre autres et dans l'optique de juguler les risques d'attaques cybernétiques au 21e siècle, de procéder à un renforcement de l'éducation des citoyens à l'usage des TIC et du dialogue public-privé, à la mise en place d'un Bureau National d'Intelligence Cybernétique, et au plan international, d'accélérer la coopération aux niveaux régional et sous régional africain par l'opérationnalisation de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo, du 27 juin 2014), les projets de lois types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et les directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC) relatives à la protection des données à caractère personnel, aux transactions électroniques et à la lutte contre la cybercriminalité.

---

[28] V. Gautrais (dir), «*Préface*», in *Droit du commerce électronique*, éd. Thémis, p. vii.

[29] Idem, p. vii.

[30] L.Pena, «*Pour une philosophie du droit universel*», 2e Colloque «*La raison juridique*»: *Mondialisation juridique et paradigmes culturels*, Madrid, 20 avril 2007, p.13.

BIBLIOGRAPHIE SELECTIVE

OUVRAGES, THÈSES ET MANUELS

1 CHR. Feral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet*, Paris, Dalloz, 4e éd., 2006.

2 L.Grynbaum, C. Le Goffic et L. Morlet –Haidara, *Droit des activités numériques*, Paris, Dalloz, 1ère édition, 2014.

3 R-E Okomen Tsague, *La dématérialisation de l'activité économique amorcée par l'AUDCG - enjeux économiques et défis juridiques dans l'espace OHADA*, Editions Universitaires Européennes, 2018, Beau Bassin. Disponible sur: *www.morebooks.fr*

4 N'Tchatat Tounya (F-L), Le cyberdroit dans l'espace OHADA, mémoire de master 2, Université de Yaoundé II, 2014

ARTICLES DE DOCTRINE, CHRONIQUES ET RAPPORTS

5 B. Benhamou, «*Les nouveaux enjeux de la gouvernance de l'internet*» In Regards sur l'actualité, Documentation française, Janvier 2007, pp.1-13.

6 Cyber cercle, «*Criminalité économique et financière à l'heure du numérique*», mis en ligne le 25 février 2015. Disponible sur: *www.cybercercle.com*

7 S. Joissains et J. Bigot , Rapport d'information (sur la lutte contre la cybercriminalité), Sénat, n°613, 09 juillet 2020, Session extraordinaire de 2019-2020.

8 INTERPOL Foundation, Cybercriminalité, Cyberbrochure, février 2017, 12 pages. Consultable sur: *www.interpol.int*

9 C. Juiff et L. Sarrat, «*Faire face ensemble: plaidoyer pour le développement d'une approche collective face aux risques cyber*», Alcyconie, 2021. Disponible sur: *https://alcyconie.com/faire-face-ensemble-plaidoyer-pour-le-developpementdune-approche-collective-face-aux-risques-cyber/*

10 C. Lequesne –Roth, «*Réseaux sociaux et contre-pouvoirs: penser les nouveaux modes de régulation*», Recueil Dalloz, 2021, p.1091.

11 E. Marique et A Strowel, «*La régulation des Fakes News et avis factices sur les plateformes*», Ride, De Boeck Supérieur, 2019, Tome XXXIII, pp.383-398.

12 Consultable sur: *http://www.cairn.info/revue-internationale-de-droit-economique-*

13 *2019-3-page-383.htm*

14 C. Morin, «*La criminalité investit le cyberespace*», Dossier Gendinfo, mise en ligne le 21 janvier 2019. Disponible sur: *www.gendinfo.fr*

15 Y. Poullet et M-N Ruffo de Calabre, «*La régulation des réseaux sociaux*», Etudes, S.E.R, Juin 2021, n°4283, pp.19-30. Consultable sur: *http://www.cairn.info/revue-etudes-2021-6-page-19.htm*

16 M. Quemener, «*Cybercriminalité: la délinquance économique du 21e siècle*», In Sécurité et Défense Magazine, 18 juillet 2015. Disponible sur: *www.SD-magazine.com*

17 P. Trudel, «*Le droit à l'information, une introduction*», article publié en ligne, p.8. Disponible sur: Lwww.pierretrudel.openum.ca/publications

L'ENCADREMENT JURIDIQUE DU CYBERESPACE

Pierre Etienne KENFACK
Professeur Agrégé des Facultés de droit
Chef du département de Théorie du droit de la Faculté des Sciences Juridiques et Politiques de l'Université Yaoundé II

INTRODUCTION

Dans les dictionnaires de la langue française, le mot espace a une dizaine de sens[1] dont trois ont fait la rencontre du droit, entendu comme discipline ou science de lecture et d'organisation du monde pour permettre la cohabitation sans conflit des personnes[2]. Dans un premier sens, l'espace désigne l'étendue, la surface ou la région. Dans un deuxième sens, l'espace désigne un domaine localisé dans lequel s'exercent certaines activités. Dans un troisième sens, l'espace désigne le milieu situé au-delà de l'atmosphère terrestre et dans lequel évoluent les corps célestes. Ces trois sens révèlent l'espace comme une notion de géométrie et de physique qui désigne une étendue, abstraite ou non, ou encore la perception de cette étendue[3]. Et c'est cette perception qui a mis le droit au contact de l'espace par soumission ou par action. La soumission du droit à l'espace résulte de ce que, du fait de la souveraineté des Etats, le droit produit par un Etat ou un groupe d'Etat n'est applicable que sur le territoire de cet Etat ou de ces Etats. L'action du droit sur l'espace résulte de ce que le droit se saisit de l'espace en posant des règles qui y sont applicables.

[1] https://www.larousse.fr/dictionnaires/francais/espace/31013
[2] J.L. Bergel, Théorie généale du droit, Dalloz, Paris,: P. Roubier, Théorie générale du droit,
[3] https://www.techno-science.net/definition/5124.html

Très tôt, le droit s'est saisi de l'espace facile d'accès à tous les hommes, notamment de l'espace terrestre en posant des règles d'organisation des rapports des personnes entre elles et avec les biens. Ainsi, chaque pays ou chaque espace juridique commun est gouverné par des blocs de règles à observer avec des procédures et mécanismes pour occuper ou exploiter une portion de l'espace et des sanctions en cas de non-respect[4]. Par la suite, lorsque les êtres humains ont atteint l'espace atmosphérique, espace difficile d'accès, le droit a aussitôt été interpellé. Ainsi, quand en 1957, l'URSS a lancé le premier satellite artificiel de la terre, il s'est immédiatement posé le problème de cohabitation dans l'espace lorsque d'autres Etats ont suivi l'exemple de cette fédération. En réponse à cette préoccupation, dans l'impossibilité d'étendre dans cette partie, les autres règles des droits des gens, les Etats ont entrepris d'instituer, au sein des Nations Unies, par des conventions internationales, un corps de règles et principes inédits qui forment aujourd'hui une branche autonome de droit appelé droit de l'espace[5]. Cette branche du droit international a pour objet la réglementation des activités des Etats dans l'espace dit «extra-atmosphérique»[6]. Sur le modèle du droit de l'espace s'est construit un droit de l'espace maritime appelé droit maritime qui régit la navigation maritime[7].

Longtemps entité simple, le mot espace s'est vu gratifié du préfixe «cyber» à l'avènement des Technologies de l'Information et de la Communication. Depuis lors on parle de «cyberespace». Que recouvre ce nouveau concept ? L'observation révèle que le mot cyberespace est un composé de «cyber» et de «espace.» Le sens du mot espace étant connu, la mise en perspective de celui de cyber est un préalable indispensable à la saisine du sens de cyber espace. Cyber signifie «un ensemble de données numérisées constituant un univers d'informations et un milieu de

[4] Ce droit est articulé autour de la distinction des systèmes juridiques, de la distinction droit public/droit privé et de la distinction droit international, droit interne.

[5] *Traités et principes des Nations Unies relatifs à l'espace extra-atmosphérique*, 2002;;

[6] A. Kerrest «Droit de l'espace. Droit des activités spatiales. Quelques définitions et remarques sur une approche pluridisciplnaire», symposium on capacity building in space law, UNCOPUOS, legal subcommittee, Vienne;, 26/27 -03 2007: F. Forster, «le droit de l'espace entre autonomie et dépendance», in, A. Bensoussan (Dir), Droit du numérique et des technologies avancées, https://www.alain-bensoussan.com/avocats/droit-de-l-espace-autonomie-dependance/2018/04/03/

[7] G. Ripert, Précis de droit maritime, Paris, Dalloz, 1942: Ph. Delebecque, Droit maritime, 14ème édit, Paris, Dalloz, 2020: A. Montas, Droit maritime, 3ème édit. Vuibert Sup Droit, 2021;

communication lié à l'interconnexion mondiale des ordinateurs». Son association avec espace a permis à des auteurs et acteurs de proposer des définitions de cyber espace.

On a ainsi défini le cyber espace comme l'espace composé d'une multitude de protocoles de communication qui mène l'information. Dans un tel sens, il est synonyme d'Internet puis de World Wide Web[8]. Un espace de communication créé par l'interconnexion des ordinateurs[9]. Prenant acte de ce que cette définition qui n'intègre pas les moyens de transmission et de données apparus après les ordinateurs ne rend pas compte de toute la richesse des mots, l'Agence Nationale de la Sécurité des Systèmes d'Information en France en a proposé une autre. D'après cette agence, le cyber espace est «l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé des données numériques»[10].

Cette définition a le mérite de prendre en compte tous les aspects techniques du cyber espace, mais l'inconvénient de ne pas mettre en perspective les activités socio-anthropologiques et juridiques qui se déroulent ou se développent sur cet espace. C'est pourquoi, mettant en exergue le cyber espace comme un lieu de rencontre et d'aventure, comme un enjeu de conflits mondiaux, un spécialiste des sciences sociales a proposé de considérer le cyberespace non seulement comme les nouveaux supports de l'information, mais également comme les modes originaux de création, de navigation dans la connaissance et des relations sociales qu'ils permettent[11].

Appelés du fait de leur mission à prendre en compte tous les aspects du cyberespace, les juristes définissent le cyberespace comme un domaine global constitué du réseau maillé des infrastructures des technologies de l'information, des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des

[8] Protocoles internet, UUCP de Usenet, protocoles de réseaux spécifiques tels que Swift ou Amadeus;
[9] Bertrand Boyer, Cyberstratégie, l'art de la guerre numérique, Paris, Nuvis, 2012, p. 104;
[10] ANSSI (2011), Défense et sécurité des systèmes d'information: une stratégie pour la France: https://www.ssi.gouv.fr/entreprise.
[11] P. Levy, *L'intelligence collective, pour une anthropologie du Cyber espace*, Paris, La Découverte, 1997

services en ligne[12]. Cette définition a le mérite de ne pas limiter le cyber espace à son aspect purement virtuel, mais de le saisir dans sa totalité, en intégrant également sa dimension réelle. Comme on l'a écrit avec beaucoup de pertinence, le cyber espace se présente en strates: une strate physique qui englobe les infrastructures du réseau des réseaux qu'est internet comprenant les serveurs racines, les bases de données, les satellites, les câbles sous-marins, les fibres optiques, une strate logique ou virtuelle comprenant les logiciels et les protocoles du réseau et une strate cognitive composée de l'ensemble des données, des informations et du contenu circulant sur le réseau[13].

Ainsi défini le cyber espace est un espace encadré sur le plan technique. Dans le cadre de l'exploitation des réseaux ou d'internet, les protocoles, codes et matériels utilisés font l'objet d'une standardisation internationale, condition essentielle de l'interconnexion des réseaux et du développement intensif d'internet[14]. Cet encadrement international au plan technique a-t-il des prolongements sur le juridique ?

Derrière cette question se profile une problématique plus générale de l'encadrement juridique du cyberespace qui est un espace par nature international. Cette problématique est inévitable compte tenu de ce que le cyber espace est un espace de cohabitation des hommes, une société et, là où il y a une société, le droit s'invite pour tenter d'organiser une cohabitation sans conflit.

De fait, les problèmes qui interpellent le droit dans le cyber espace sont nombreux et variés. Les plus visibles concernent l'accès et le maintien dans cet espace, le traitement des données de ceux qui accèdent ou se déploient dans cet espace, l'exercice des droits et libertés dans cet espace, la moralisation de cet espace, les responsabilités et la réparation des dommages causés par les utilisateurs de l'espace etc. Le droit s'invitant en tout lieu où des personnes cohabitent, n'a pu rester indifférent en présence du cyber espace et a dû s'en

[12] B. Louis-Sidney , «La dimension juridique du cyber espace», Revue Internationale et Stratégique, n°87, 2013/3, pp. 73 et s. CCD-COE (2013), Manuel de Tallin de droit international applicable à la cyberguerre, Cambridge University press, Cambridge, www.ccdcoe.org; O. Barat-Ginies , «Existe-t-il un droit international du cyberespace», https://www.cairn.info/revue-herodote-2014-1-page-201.htm

[13] B. Boyer, *Cyberstratégie, l'art de la guerre numérique*, Paris, Nuvis, 2012, p. 104B.

[14] B. Louis-Sidney, «la dimension juridique du cyber espace», *Revue internationale et stratégique*, n°87, 2012/3 , pp.73 et s.

saisir et l'encadrer. Mettre en perspective cet encadrement est l'objet de cette contribution qui considère deux questions majeures.

La première est de savoir quelle est l'origine des règles d'encadrement du cyber espace ? La question a opposé les partisans de la création d'un droit sui generis du cyber espace de source et d'application totalement internationales et ceux de l'indépassable souveraineté des Etats qui suggèrent l'adaptation des mécanismes classiques de production des normes au cyberespace[15]. Elle a été très facilement réglée du fait de l'inexistence d'un législateur international capable de poser des règles transcendant les frontières et susceptibles d'obliger les Etats sans leur accord et par le caractère essentiellement territorialiste des modalités d'accès des acteurs au cyberespace. De ce fait, la construction du droit du cyber espace n'a pas dérogé au mécanisme classique de production des normes portant sur les questions comportant un élément d'extranéité qui articule conventions internationales et droit interne des Etats. Ainsi, malgré l'existence des conventions internationales régissant le cyberespace, la production ou l'accueil des règles d'encadrement du cyberespace reste de la compétence de chaque Etat souverain. Comme on l'a écrit avec beaucoup de pertinence: «l'émergence d'une société de l'Information planétaire depuis le Sommet de Genève a provoqué une intensification de la réglementation étatique en vue de créer un véritable ordre public numérique à l'échelle locale et les instruments institutionnels et normatifs destinés à assurer sa protection. De ce fait, les autorités administratives et le juge ont été mis à contribution dans un processus d'adaptation ou de révolution selon l'objet à réguler en relation avec les TIC»[16].

Malgré le caractère planétaire du cyberespace, c'est finalement du côté des chaque Etat souverain qu'il faut observer les modalités d'encadrement du cyberespace. Notre for d'observation étant le Cameroun, c'est en scrutant le droit positif de ce pays qu'il a fallu rechercher les éléments de réponse à la seconde question qui est apparue plus complexe et sur laquelle a été bâtie cette contribution.

---

[15] O. Barat-Ginies, «existe-t-il un droit international du cyber espace ?», https://www.cairn.info/revue-herodote-2014-1-page-201.htm; F. AJINA, Cadre juridique de la cybersécurité dans l'espace francophone, AUF/IFUC, https://pssis.sec.gouv.sn/sites/default/files/cadre%20juridique%20_0.pdf; Master Droit du cyberespace africain, Cours M1b: Sources du droit du cyberespace, http://196.1.99.9/moodle/mod/book/print.php?id=62;

[16] Master Droit du cyberespace africain, Cours M1b, sources du droit du cyber espace op. cit.

Que prévoit le droit positif camerounais pour l'encadrement du cyberespace ? Pour rechercher des éléments de réponse à cette interrogation l'analyse de toutes les règles positives d'origine internationale ou interne applicables au cyberespace au Cameroun est apparue indépassable. Elle a mis en perspective un encadrement juridique du cyberespace tenant compte de la distinction entre l'accès au cyberespace qui combine des éléments matériels avec les éléments virtuels et la vie dans cet espace constituée d'éléments essentiellement virtuels. Ce qui nous a conduit construire cette réflexion autour de deux axes: L'encadrement juridique de l'accès au cyberespace (I) d'une part, et l'encadrement juridique des activités dans le cyberespace (II), d'autre part.

I - L'ENCADREMENT JURIDIQUE DE L'ACCÈS AU CYBER ESPACE

Bien que le cyberespace soit un espace planétaire, l'entrée n'y est pas libre. Le régime juridique de l'entrée est dominé par deux impératifs majeurs: permettre à toute personne se trouvant ou ayant attache avec un territoire d'accéder à l'espace virtuel d'une part, faciliter l'identification et la sanction des auteurs des perturbations ou des actes malveillants sur le cyber espace d'autre part. En l'absence d'une structure mondiale pouvant faciliter l'identification et la sanction des auteurs des actes malveillants et des perturbations sur le cyberespace, c'est chaque Etat qui a la responsabilité de s'en charger. Chaque Etat organise les modalités d'entrée des personnes se trouvant sur son territoire ou ayant une attache avec son territoire dans le cyber espace. L'encadrement juridique de l'accès au cyberespace poursuit deux objectifs majeurs. L'encadrement de l'accès au cyberespace est organisé au Cameroun par la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014 à Malabo, la loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun modifiée par la loi N°2015/06 du 20 avril 2015, la loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun, la loi N°2010/021 du 21 décembre 2010 régissant le commerce électronique au Cameroun , le décret N°2019/150 du 22 mars 2019 portant organisation et fonctionnement de l'Agence Nationale des Technologies de l'Information

et de la Communication. Ces textes mettent en place un régime d'accès au cyber espace articulé autour de deux principaux pôles: la consécration d'un droit d'accès de toutes les personnes au Cyber espace (A) et le contrôle par l'Etat de tout le processus d'accès au cyberespace (B).

A. LA CONSECRATION D'UN DROIT D'ACCES DE TOUTES LES PERSONNES AU CYBERESPACE

L'importance du cyberespace pour la vie économique, sociale et culturelle des personnes a conduit le législateur camerounais à proclamer et à poser des mécanismes de mise en œuvre d'un droit d'accès au cyberespace dans la loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun. La proclamation est faite par l'article 4 de ce texte qui dispose que: «toute personne a le droit de bénéficier des services de communications électroniques, quelle que soit sa localisation géographique sur le territoire national». Ce texte pose le principe d'après lequel toute personne physique ou morale, publique ou privé a le droit d'accéder au cyber espace. Pour permettre la mise en œuvre de ce droit, le texte a institué un service universel et un processus de développement des communications électroniques sur le territoire camerounais.

L'article 5 définit le service universel comme «ensemble minimal des services définis de bonne qualité qui est accessible à l'ensemble de la population dans les conditions tarifaires abordables indépendamment de la localisation géographique» et l'article 28 alinéa 1 du texte en fait une obligation à la charge de l'Etat en ces termes: «l'obligation de service universel des communications électroniques couvre la fourniture à tous, des services de communications électroniques de bonne qualité, à des conditions tarifaires abordables, et de façon ininterrompue». L'obligation de service universel met à la charge de l'Etat un ensemble de charges incompressibles et ouvre en faveur des personnes des droits et libertés conformément à la loi 2010/013 du 21 décembre 2010 régissant la communication électronique. Relativement aux charges, l'obligation de service universel impose à l'Etat, conformément à l'article 27:

- D'ouvrir à tous la possibilité de raccordement au réseau téléphonique public;

- de mettre à disposition des points d'accès aux services de communications électroniques;
- de permettre l'accès aux services d'urgence;
- d'assurer aux groupes sociaux vulnérables des mesures particulières;
- d'assurer l'acheminement des communications électroniques en provenance et à destination des points d'abonnement;
- d'assurer l'acheminement gratuit des communications électroniques d'urgence;
- d'assurer la fourniture d'un annuaire universel d'abonnés imprimé et électronique et d'un service de renseignement gratuit;
- d'assurer toute autre activité du secteur des télécommunications et des technologies de l'information et de la communication arrêtée par les pouvoirs publics.

Relativement aux droits et libertés, d'après l'article 28 de la loi de 2010, l'obligation de service universel ouvre en faveur des personnes:

- La faculté de pouvoir être raccordé aux réseaux publics et d'avoir accès aux services de base de communications électroniques;
- Le bénéfice des autres services de communications électroniques selon la zone de couverture de chaque service;
- L'accès aux informations de base relative aux conditions;
- La liberté de choix du fournisseur des services de communications électroniques;
- L'égalité d'accès aux services de communications électroniques;
- L'accès aux informations de base relatives aux conditions de fourniture des services de communications électroniques et leur tarification.

Ces obligations imposées à l'Etat, les droits et libertés accordés aux personnes consacrent un droit d'accès au cyberespace, mais un droit contrebalancé par la nécessité d'éviter que le cyberespace ne devienne un espace de délinquance où les acteurs sont invisibles. C'est pourquoi, ce droit d'accès est limité par un contrôle de l'accès au cyberespace.

B. LE PLACEMENT SOUS LE CONTROLE DE L'ETAT DE TOUT LE PROCESSUS D'ACCES AU CYBERESPACE

Le cyberespace tout en étant un espace utile et libre est un espace dangereux pour les Etats et pour les droits et libertés des personnes. Il est susceptible d'accueillir et abriter des cybers délinquants qui peuvent facilement se dissimuler dans un espace aussi ouvert. La seule possibilité de les rechercher est de recourir à leur identification lors de leur entrée à travers l'exigence des coordonnées de tous les entrants dans cet espace. C'est ce que font les législateurs de tous les Etats en plaçant tout le processus d'accès au cyberespace sous le contrôle de l'Etat. La loi camerounaise N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, modifiée par la loi N°2015/06 du 20 avril 2015 ne déroge pas à cette exigence en plaçant l'Etat à la tête de tout le processus d'accès au cyberespace en lui donnant compétence exclusive pour l'institution des points d'entrée et pour assurer le contrôle de l'activité des points d'entrée.

Relativement à l'institution des points d'entrée la loi fait la différence entre l'installation des équipements et l'accueil des fournisseurs d'accès.

La compétence exclusive de l'Etat sur l'installation des équipements permettant l'accès au cyber espace sur son territoire est posée par l'article 6 alinéa 2 de la loi n° 2010/013 du 21 décembre 2010 modifiée en 2015 qui dispose: «relèvent de la compétence de l'Etat et peuvent faire l'objet de concessions:

- La construction et l'exploitation sur toute l'étendue du territoire national des points d'atterrissement des câbles sous-marins;
- La construction et l'exploitation vers des téléports vers un ou plusieurs réseaux satellites;
- L'établissement et l'exploitation des multiplex et des réseaux de diffusion.

En ce qui concerne l'accueil des fournisseurs d'accès, la compétence de l'Etat pour l'installation des fournisseurs d'accès découle de plusieurs articles de la loi qui permet à l'Etat d'accorder des concessions, des licences et des agréments. Les concessions sont octroyées pour: «l'établissement et

l'exploitation des communications électroniques à couverture nationale ouvert au public, l'établissement et l'exploitation des réseaux de transport des communications ouverts au public» (art.9). Quant aux licences, elles sont octroyées aux personnes physiques et morales pour établir et exploiter notamment: «tout service support, les réseaux radioélectriques… , les réseaux privés indépendants, les réseaux temporaires, les réseaux expérimentaux, les réseaux de collecte et/ou de distribution en vue de la fourniture au public des services de communications électroniques, les réseaux de communications ouverts au public dans les zones rurales, les réseaux virtuels ouverts au public, les infrastructures passives en support aux réseaux de communications électroniques».

Les agréments sont octroyés aux personnes physiques et morales:

- L'exercice de l'activité d'installation des équipements et infrastructures des communications électroniques;
- Les laboratoires d'essai et mesures des équipements de communications électroniques;
- La vente des équipements des communications électroniques.

Les titulaires de ces titres sont astreints à l'obligation de procéder à l'identification de toutes les personnes qu'elles introduisent sur le cyberespace par leurs activités. C'est ce qui ressort de l'article 55 de la loi de 2010 qui dispose: «les opérateurs et exploitants des réseaux de communications ouverts au public, ainsi que les fournisseurs de services sont tenus, au moment de toute souscription de procéder à l'identification des abonnés et des terminaux. Ils tiennent à jour les listes des abonnés».

Relativement au contrôle de l'activité des points d'entrée, la compétence exclusive de l'Etat découle de l'institution par la loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun, modifiée par la loi N°2015/06 du 20 avril 2015 d'un régulateur des services des télécommunication appelé Agence de Régulation des Télécommunications (ART) et d'une agence chargée de la régulation, du contrôle et du suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques (ANTIC).

D'après l'article 36 de ce texte, la régulation, le contrôle et le suivi des

activités des opérateurs et fournisseurs des services de communications électroniques sont assurés par une agence de régulation. L'agence a plusieurs missions dont l'une des plus importante est la facilitation de l'identification des personnes accédant au cyber espace. D'après l'article 49 du texte, l'Agence établit et gère le plan national de numérotation et d'adressage. Ce plan détermine l'ensemble des adresses et numéros permettant d'identifier les points de terminaison des réseaux et des services de communications électroniques, d'acheminer les appels et d'accéder aux ressources internes des réseaux, conformément aux recommandations de l'Union Internationale des Télécommunications. Elle garantit un accès égal et simple des utilisateurs aux différents réseaux et services ainsi que l'équivalence des formats de numérotation. D'après l'article 50, l'Agence de régulation attribue dans des conditions objectives, transparentes et non discriminatoires aux opérateurs qui demandent des adresses, des préfixes et des numéros moyennant une redevance. L'article 96 qui crée l'ANTIC lui donne plusieurs missions dont certaines contribuent à la facilitation de l'identification des acteurs se trouvant dans le cyber espace. D'après ce texte, l'ANTIC a pour mission entre autres d'élaborer la politique et les procédures d'enregistrement des noms de domaines «.cm», de l'hébergement, de l'administration des serveurs racine, de l'attribution d'agrément de Registrar, du «.cm»: - de planifier, d'attribuer et de contrôler les adresses Internet (IP) au Cameroun: de mettre en place des mécanismes pour assurer la sécurité de l'Internet au niveau national.

Cette volonté de faciliter l'identification des acteurs du cyberespace est réaffirmée par les missions assignées à cet organisme par la loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la lutte contre la cybercriminalité au Cameroun. D'après l'article 7 de ce texte, l'ANTIC a, parmi ses missions, celles:

- d'instruire les demandes d'accréditation et de préparer les cahiers de charges des autorités de certification et de les soumettre à la signature du Ministre chargé des Télécommunications;
- de contrôler la conformité des signatures électroniques émises;
- d'instruire les demandes d'homologation des moyens de cryptographie et de délivrer les certificats d'homologation des équipements de sécurité;

- d'assurer la veille technologique et d'émettre des alertes et recommandations en matière de sécurité des réseaux de communications électroniques et de certification;
- d'assurer la surveillance, la détection et l'information aux risques informatiques et cybercriminels.

Faciliter l'accès au cyber espace en prenant des précautions pour faciliter l'identification des acteurs qui s'y trouvent est l'orientation choisie par le Cameroun pour encadrer l'entrée dans le cyberespace. Quelle est celle de l'encadrement des activités dans le cyber espace.

II - L'ENCADREMENT JURIDIQUE DES ACTIVITÉS MENÉES DANS LE CYBER ESPACE

Le cyberespace est un lieu d'exercice d'activités variées. On y retrouve des activités de communication, de commerce, d'échanges de biens et services etc. L'encadrement de telles activités qui ne sont inconnues des droits positifs des Etats ne concerne que les situations où elles ne sont pas prises en compte par les règles de droit déjà disponibles. La plupart de ces activités n'étant pas des innovations dans le cyber espace sont régies par le droit commun. Mais pour celles qui sont nées ou se sont accentuées grâce au cyber espace, le droit commun ne suffisait plus et ne pouvait venir qu'en complément des règles spéciales. C'est pourquoi le législateur camerounais s'est empressé de les encadrer en édictant des règles dérogatoires à celles du droit commun (A) ou des règles sans lien avec celles de droit commun (B).

A - L'ENCADREMENT DES ACTIVITÉS MENÉES DANS LE CYBERESPACE PAR DES RÈGLES DÉROGATOIRES À CELLES DU DROIT COMMUN

Les règles dérogatoires à celles du droit commun sont celles qui sont édictées pour régler des questions déjà traitées par les règles en vigueur. Elles sont contenues dans des textes dits spéciaux. Les textes spéciaux

édictés depuis l'avènement du cyberespace en complément des règles de droit commun encadrent, le commerce électronique (1) et les communications électroniques (2).

1 - L'ENCADREMENT DU COMMERCE ÉLECTRONIQUE

L'encadrement du commerce électronique est assuré par la loi N°2020/021 du 21 décembre 2010. Ce texte qui vient en complément du Code civil, du code de commerce et des lois sur la concurrence et la protection des consommateurs, pose des principes régissant l'exercice des activités relatives au commerce électronique, organise le régime de la responsabilité des prestataires et des intermédiaires, indique les modalités d'authentification et de sécurisation des données et des renseignements et contient quelques dispositions pénales spéciales.

Relativement aux principes, après avoir rappelé le principe de la liberté de commerce, la soumission de l'activité de commerce électronique aux normes générales relatives à l'exercice des activités commerciales, le texte exclut certaines matières de son champ d'application: les jeux d'argents et des paris légalement autorisés, les activités de représentations et d'assistance en justice, les activités exercées par les notaires[17]. Le texte fixe le régime de la publicité par voie électronique[18], les modalités de conclusion des contrats par voie électronique[19], le régime des transactions électroniques[20].

Relativement au régime de la responsabilité des prestataires et intermédiaires, le texte met à la charge de toute personne qui exerce une activité de commerce électronique une obligation spéciale d'information visant à assurer aux destinataires des services et des autorités un accès facile et direct aux informations sur l'identité du prestataire, sa situation vis-à-vis du registre de commerce, les modalités de son accès à l'activité[21]. Il indique les conditions spéciales d'engagement de la responsabilité des personnes qui exercent l'activité de stockage, de conservation et de transmission des données par voie électronique[22]. Concernant à la

[17] Article 3
[18] Articles 5 et suivants.
[19] Articles 9 et suivants
[20] Articles 15 et suivants.
[21] Articles 30 et suivants

sécurisation et à l'authentification des données et des renseignements, le texte permet à toute personne physique ou morale de recourir au certificat et à la signature électronique et précise les conditions d'utilisation[23]. Quant aux dispositions pénales spéciales, le texte crée des infractions spéciales à l'exercice des activités de commerce électronique avec les sanctions correspondantes et un régime spécial de répression. Outre le commerce électronique, le législateur camerounais a posé des règles dérogatoires au droit commun pour encadrer les communications électroniques.

2 - L'ENCADREMENT DES COMMUNICATIONS ÉLECTRONIQUES.

Les communications électroniques sont celles qui se font essentiellement dans le cyberespace. Leur encadrement juridique au Cameroun est organisé par la loi N°2010/013 du 21 décembre 2010 régissant les communications électroniques au Cameroun. Ce texte qui déroge aux textes généraux sur la communication au Cameroun fixe le régime juridique des réseaux et des communications électroniques, institue un service universel du développement des activités économiques, organise la règlementation, la régulation et le contrôle des communications électroniques et institue un système de règlement du contentieux dans le domaine des communications électroniques.

Le régime des réseaux et des communications électroniques fait l'objet du titre 2 qui après avoir fait de l'Etat le gestionnaire exclusif du spectre des fréquences et des positions orbitales nationales, précise que l'autorisation et la déclaration sont les régimes de l'établissement et ou de l'exploitation des réseaux et de la fourniture des services de communication électronique. Le texte indique les types d'autorisation et détaille leur régime juridique: la concession, la licence et l'agrément de chaque. Le titre indique également les activités soumises au régime de la déclaration, les conditions et les modalités de la déclaration.

Le titre 3 du texte institue un service universel du développement des communications électroniques, en le définissant comme un «ensemble minimal des services définis de bonne qualité qui est accessible à

[22] Articles 33 et suivants.
[23] Articles 35 et suivants.

l'ensemble de la population dans les conditions tarifaires abordables indépendamment de la localisation géographique». Le titre précise l'objet du service universel, les modalités de son ancrage sur le territoire et indique les modalités de développement des communications électroniques et celles de financement de ces activités.

Le titre 4 consacré à la règlementation à la régulation et au contrôle des activités de communications électroniques indique la politique de développement du secteur des télécommunications et des technologie de l'information et de la communication de l'Etat camerounais, organise la régulation et le suivi des activités des opérateurs et des fournisseurs des services de communications électroniques, fixe le régime de gestion du spectre des fréquences , celui de l'interconnexion des réseaux et du partage des infrastructures, indique le processus de numérotation et d'adressage, organise le processus de protection des consommateurs des produits des communications électroniques. Les titres 5 et 6 précisent le régime des servitudes des communications électroniques et organisent la gestion du contentieux entre opérateurs et le régime de la répression des infractions. En plus de ces règles dérogatoires au droit commun, le législateur camerounais encadre les activités menées dans le cyberespace par des règles sans lien avec celles de droit commun.

B - L'ENCADREMENT DES ACTIVITÉS MENÉES DANS LE CYBERESPACE PAR DES RÈGLES SANS LIEN AVEC CELLES DE DROIT COMMUN

Les règles juridiques sans lien avec celles de droit commun sont celles qui régissent les questions non abordées par le droit commun, qui se préoccupent des questions nées à l'occasion du développement du cyberespace. Elles se préoccupent de la sécurité des réseaux des communications électroniques et des systèmes d'information. Elles sont contenues dans la loi N° 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité au Cameroun. Ce texte organise l'encadrement juridique de la cybersécurité (1) de la cybercriminalité (2) au Cameroun.

1 - L'ENCADREMENT JURIDIQUE DE LA CYBERSÉCURITÉ

La cybersécurité désigne d'après ce texte, l'«ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes». Son régime juridique fait l'objet de tout le titre 2 de la loi. Ce texte qui affiche dès son entame la politique générale de sécurité électronique, fixe le régime de la régulation et du suivi des activités de sécurité électronique et le processus de protection et de sécurisation des activités électroniques et des systèmes d'information.

La régulation et le suivi des activités de sécurité électronique font l'objet des articles 7 et suivants. L'article 7 confie à l'Agence Nationale des Technologies de l'Information et de la Communication instituée par la loi sur la communication électronique, la mission de réguler, en collaboration avec l'Agence de Régulation des Télécommunications les activités de sécurité électronique sur le territoire camerounais. A cet effet, l'Agence assure pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques, et à la certification électronique. Elle est l'autorité de certification racine et de l'administration publique.

Le processus de protection et de sécurisation des activités électroniques et des systèmes d'information fait l'objet des articles 24 et suivants qui imposent aux opérateurs des réseaux de communications électroniques et aux fournisseurs des services de communications électroniques l'obligation de prendre toutes les mesures techniques et administratives nécessaires pour garantir la sécurité des services offerts: conserver les données de connexion et de trafic pendant une période de dix (10) ans et d'installer des mécanismes de surveillance de trafic des données de leurs réseaux.

Les mêmes textes imposent aux exploitants des systèmes d'information de: prendre toutes les mesures techniques et administratives afin de garantir la sécurité des services offerts. A cet effet, ils se dotent de systèmes

normalisés leur permettant d'identifier, d'évaluer, de traiter et de gérer continûment les risques liés à la sécurité des systèmes d'information dans le cadre des services offerts directement ou indirectement. De mettre en place des mécanismes techniques pour faire face aux atteintes préjudiciables à la disponibilité permanente des systèmes, à leur intégrité, à leur authentification, à leur non répudiation par des utilisateurs tiers, à la confidentialité des données et à la sécurité physique. Le même texte de loi organise l'encadrement juridique de la cybercriminalité au Cameroun.

2 - L'ENCADREMENT JURIDIQUE DE LA CYBERCRIMINALITÉ

Le mot cybercriminalité n'est pas juridique. C'est un mot qu'on retrouve dans le dictionnaire de la langue française et qui désigne toute infraction commise en utilisant un réseau d'ordinateur ou d'Internet[24]. La loi de 2010 la définit comme «ensemble des infractions s'effectuant à travers le cyberspace par d'autres moyens que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique». Cette définition qui n'est pas éloignée de celle des dictionnaires de la langue française rappelle que ce sont des infractions qui n'existent qu'à l'occasion d'une activité dans le cyber espace. Son régime juridique, totalement détaché du droit commun est fixé au Cameroun par le titre 3 de la loi de 2010 et se singularise surtout par la procédure.

Le texte donne compétence à la fois aux Officiers de Police à compétence générale et aux Officiers de Police Judiciaire à compétence spéciale pour rechercher les infractions et les délinquants en ces termes: «les Officiers de Police Judiciaire à compétence générale et les agents habilités de l'Agence, procèdent aux enquêtes conformément aux dispositions du Code de Procédure Pénale». Il autorise des perquisitions portant à la fois sur les données virtuelles et les supports physiques: «Les perquisitions en matière de cybercriminalité sont susceptibles de porter sur des données qui peuvent être des supports physiques ou des copies réalisées en présence des personnes qui assistent à la perquisition». Il accorde aux autorités judiciaires camerounaises le pouvoir de donner une commission rogatoire tant nationale qu'internationale, à toute personne morale ou

[24] Dictionnaire Le Robert

physique pour rechercher les éléments constitutifs des infractions de cybercriminalité, dont au moins l'un des éléments constitutifs a été commis sur le territoire camerounais ou dont l'un des auteurs ou complices se trouve sur le territoire camerounais.

Il oblige les personnes physiques ou morales qui fournissent des prestations de cryptographie visant à assurer une fonction de confidentialité, à remettre aux Officiers de Police Judiciaire ou aux agents habilités de l'Agence, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies.

CONCLUSION

Bien que virtuel, le cyberespace a une base physique qui a un impact indéniable sur son encadrement juridique. En effet, malgré son caractère mondial, l'encadrement du cyberespace n'est possible qu'à partir d'un espace territorial donné qui est essentiellement étatique. Outre les questions de souveraineté, cette démarche s'impose parce que l'accès à cet espace n'est possible qu'à partir d'un point localisé sur un territoire. La prise en compte de cette donnée fondamentale permet d'anticiper sur la recherche des responsables des dommages causés dans cet espace et la sanction des perturbateurs du fonctionnement de cet espace en n'autorisant l'entrée qu'à des personnes préalablement identifiées. Ce n'est certes pas une garantie absolue, mais l'analyse du dispositif d'encadrement juridique du cyberespace à partir du Cameroun nous laisse observer que c'est la seule voie disponible pour l'instant produisant des résultats probants.

RAPPORT GENERAL DES TRAVAUX DU COLLOQUE SUR LE THEME : «MEDIACRATIE CYBERNETIQUE ET MENACES SECURITAIRES: ENJEUX, DEFIS ET REPONSES A L'ERE DE LA DIGITALISATION»

Bernard-Raymond GUIMDO DONGMO
Professeur Titulaire (CAMES) des Universités

INTRODUCTION

Dans le cadre de la mise en œuvre de ses missions statutaires en matière de formation et de recherche sur les questions relatives à la sécurité et le maintien de la paix, l'Ecole Internationale des Forces de Sécurité (EIFORCES) a organisé, les 28 et 29 avril 2022, un Colloque international sur le thème: **«Médiacratie cybernétique et menaces sécuritaires: enjeux, défis et réponses à l'ère de la digitalisation».**

A l'occasion de cette grand-messe scientifique, une large et riche palette de participants a été mobilisée, comprenant les Forces de Défense et de Sécurité, les universitaires, les chercheurs et experts de haut vol, les spécialistes des cyber-sciences et des TIC, les autorités administratives, les membres de la société civile, la communauté étudiante, les représentants des Organisations Internationales, les Représentants des Pays Partenaires.

Le cadre, les moyens et les conditions de travail adéquats, dont ils ont pu bénéficier, ont favorisé un rendement collectif optimal. Des postures, renforçant

l'intérêt du débat contradictoire, incluant la liberté de ton, l'écoute, la courtoisie, les piques, le partage d'idées, ont ainsi pu être observées et appréciées. Une rencontre de plus ou une rencontre de trop ? Des discours savants de plus ou de trop ? Que non ! On a eu droit à une rencontre à la fois utile, utilitaire et utilisable.

Au demeurant, deux temps forts ont ponctué cette rencontre internationale: **la cérémonie d'ouverture** et **les travaux des quatre panels**, ponctués d'**échanges interactifs**.

Relativement à la cérémonie d'ouverture, elle a été marquée par le Mot du Général de Brigade, Directeur Général de l'EIFORCES, André Patrice BITOTE, l'Allocution d'ouverture du Ministre Délégué à la Présidence de la République, chargé de la Défense, Joseph BETI ASSOMO, la Présentation des différentes articulations du Colloque et des résultats attendus par le Dr PASSO SONBANG Elie, Commissaire Divisionnaire, Chef du Centre de Recherche et de la Documentation de l'EIFORCES, enfin, la Leçon inaugurale du Pr Laurent-Charles BOYOMO ASSALA, Modérateur Général des travaux.

- Dans son propos de circonstance, **le Général de Brigade, Directeur Général de l'EIFORCES, André Patrice BITOTE** a tenu à signaler la présence à ces travaux, des auditeurs du BESS, présence qui constitue la preuve de la symbiose qui existe entre les pôles Formation et Recherche qui structurent le déploiement de l'EIFORCES en tant que Centre d'Excellence dans les matières liées à la sécurité et au maintien de la paix. Ce déploiement est d'autant plus encouragé par les pouvoirs publics camerounais en général, et le Président de la République en particulier, qui a donné son onction aux présentes assises, en permettant le financement endogène de ce rendez-vous de la science consacré à une thématique aussi actuelle que pertinente. Ladite thématique, dédiée à **la médiacratie cybernétique,** s'inscrit d'ailleurs, dans le prolongement de la réflexion engagée quelques années plus tôt par l'EIFORCES, avec le soutien du Japon à travers le PNUD, sur le thème «Défis et Enjeux de la Cybercriminalité et de la Cybersécurité en Afrique Centrale». Toute chose qui achève de convaincre de l'intérêt qu'il suscite chez les décideurs camerounais et auprès des pays et organisations partenaires.
- Cette attention particulière a été rappelée, fort opportunément, par **le Ministre Délégué à la Présidence de la République, chargé de la Défense, Joseph BETI ASSOMO**. Pour l'orateur, si

l'appropriation rapide des outils numériques est une évidence à l'époque contemporaine, les dérives inhérentes à leur utilisation inappropriée se sont également démultipliées, à l'instar des «*fake news*», des attaques cybernétiques, des discours haineux ou encore de la violence verbale distillée à travers les réseaux sociaux. Avec l'avènement des médias cybernétiques a-t-il souligné, on peut déplorer la dilution de l'éthique et la non prise en compte des critères de validité d'une information de qualité que sont l'exactitude, la justesse et la sincérité et ce, en dépit des appels répétés à un usage responsable des médias sociaux, notamment par la jeunesse, principale catégorie de consommateurs des produits numériques. L'actualité et la sensibilité du présent Colloque, a-t-il relevé, le situe résolument au cœur d'une problématique devenue structurante à l'ère de la mondialisation et de la virtualisation des échanges et des menaces. L'optique visé, pense-t-il, est de contribuer à une meilleure compréhension des concepts opératoires et des applications y afférentes, pour la formulation des solutions à la fois efficaces et pérennes à menaces sécuritaires induites.

- La présentation des activités du Colloque, faite par **le Commissaire Divisionnaire PASSO SONBANG Elie, Chef du Centre de Recherche et de Documentation de l'EIFORCES**, a pour sa part, et au-delà des précisions épistémologiques et méthodologiques et des indications sur l'articulation des panels, mis une emphase sur l'impératif de la coordination des intelligences différentielles pour une meilleure prise en charge des diverses problématiques attachées à l'encadrement des usages des technologies digitales et la lutte contre les cybermenaces.
- La leçon inaugurale, prononcée par **le Pr Laurent-Charles BOYOMO ASSALA**, a permis de mettre en lumière un certain nombre de questions structurantes qui interrogent non seulement la manière par laquelle le nouvel espace virtuel prend sens en Afrique contemporaine, mais également la nature des contours d'une nouvelle citoyenneté remodelée par la virtualité et les incidences d'une digitalisation, pas toujours appréhendée de manière adéquate, sur les configurations sécuritaires actuelles. Paradoxalement, en dépit de la prétention à l'universalité du cyberespace, la fracture numérique a exacerbé la division, voire la hiérarchisation internationale du contrôle de la connaissance scientifique et technique. Force est de relever, en effet, a souligné l'orateur, qu'à rebours du principe de liberté et de l'idéal d'émancipation des peuples,

l'imaginaire cybernétique est aujourd'hui porteur d'une certaine radicalité et d'utopies (utopies liées à l'avènement d'évidences pas toujours vraies: utopie d'un cybermonde enchanté, espace de création et d'innovation, de liberté et d'expression, etc.)

- Pour l'intervenant, dans ce monde qui, au premier abord, suscite un enchantement réel, la nouvelle économie numérique créative et libérale se pose, aux côtés d'une nouvelle cyber citoyenneté affranchie des limitations spatiales, comme un axe majeur. Ce faisant, ces axes n'en occultent pas, du seul fait de leur existence, le risque totalitaire des systèmes de fonctionnement, des hiérarchies du savoir et des fractures qui y sont à l'œuvre. Selon l'orateur, la division demeure du point de vue du partage inégalitaire de la connaissance, qui consacre une fois encore, la place marginale de l'Afrique dans le concert désormais virtualisé des nations modernes. A ce stade, le vivre-ensemble égalitaire, sur la base digitale, peut apparaître lui aussi comme une utopie, un imaginaire mobilisé à des fins dont l'évidence n'est pas toujours celle que l'on croit. La tentation peut être alors de résumer l'univers cybernétique à cette dimension instrumentale, lui déniant son ancrage socio-historique et la réalité d'un vrai champ de contradictions, de compétitions, voire de défiance, où les idéologies favorables cohabitent avec celles plus réactionnaires. L'optique n'est pas, somme toute, de faire le choix du rejet de ce nouveau monde cybernétique, mais de **le retourner sur lui-même**, afin d'en faire un vaste laboratoire de «reconceptualisation» et de réajustements travaillant pour l'intérêt commun.

Après cette Leçon inaugurale, fort consistante et porteuse de rêve et d'espoir, après le désespoir évoqué, puis révoqué, quatre Modérateurs ont, tour à tour, sous la supervision du Pr BOYOMO ASSALA Laurent Charles, coordonné les exposés et les échanges dans leurs panels respectifs, à savoir: le Pr MINKOA SHE Adolphe, Recteur de l'Université de Yaoundé II Soa **(Panel 1: La nouvelle donne insécuritaire à l'ère du numérique et des médias sociaux)**, le Pr BOYOMO ASSALA Laurent Charles lui-même **(Panel 2: Médias sociaux et numérisation: dilemme»risque-opportunité» sécuritaire)**, le Pr ANOUKAHA François, Vice-président de la CONAC **(Panel 3: Internet et médias sociaux: de l'état de nature à l'ordre)**, et le Pr OLINGA, Alain Didier Conseiller technique au Ministère de la Défense **(Panel 4: Quel avenir sécuritaire, quelle communication et quel**

développement à l'ère des menaces liées à la médiacratie cybernétique).

Toutes les communications présentées dans le cadre de ces panels ont tenté de répondre à la question suivante: **La médiacratie cybernétique est-elle ou pas un facteur de développement des menaces sécuritaires à l'ère de la digitalisation ?** L'idée forte qui s'est dégagée de ces différentes communications est que **la médiacratie cybernétique est une variable avec laquelle il va inévitablement falloir composer en la retournant sur elle-même pour lui donner un visage humainement et socialement acceptable.**

Pour rendre compte de cette idée forte, plusieurs angles d'approches étaient mobilisables, voire possibles et plausibles. Mais il nous a semblé que le plus fécond, parce qu'il tient compte de la substance et de la portée des communications présentées, consistait à montrer ou démontrer d'une part **l'impérium actuel du chamboulement cybermédiatique (I)**, et, d'autre part, **la nécessité de maîtriser ce chamboulement (II)**. Cette double considération a permis de déboucher sur la formulation **des éléments de perspective que sont les recommandations.**

I- L'IMPERIUM DU CHAMBOULEMENT CYBERMEDIATIQUE

Le boom du numérique, avatar de la globalisation, est un outil dans la fabrique des perceptions et de la puissance. L'Afrique, nouveau *«territoire du numérique»,* peine à investir pleinement ce secteur à cause de son faible investissement infrastructurel, alors qu'à contrario, elle occupe une place de choix dans l'industrie cybercriminelle. Et pourtant, telle une pieuvre (A), qui ne cesse d'étendre ses tentacules dans tous les secteurs de la vie, la médiacratie cybernétique, outil au double visage mi-ange et mi-démon, tente de s'imposer, avec ses avantages et inconvénients, et de prendre progressivement la figure d'une hydre (B).

A- L'AVENEMENT DE LA PIEUVRE CYBERMEDIATIQUE

A l'ère de la mondialisation, l'internet et les médias sociaux se sont progressivement positionnés comme des instruments structurants de la démocratie participative et délibérative, avec une certaine libéralisation de la revendication, voire de la défiance sociétale **(Pr Alice NGA MINKALA)**. Il

en résulte une reconfiguration de l'espace public et une redéfinition de l'échelle des valeurs sociales et, partant, sécuritaires.

Cette libéralisation trouve, dans le cyberespace, sa consécration totale, en tant qu'espace sans frontière et infini, poreux et fugace, qui échappe facilement à la régulation (**M. Prosper DJOURSOURBO PAGOU**).

Le taux de pénétration mondiale de l'internet est sans cesse grandissant, avec la montée en puissance des vecteurs de communication et d'échange dématérialisés **(M. Prosper DJOURSOURBO PAGOU**). Comme dans l'espace physique, qui a des acteurs dominants, le cyberespace a aussi les siens. Pur hasard ou simple coïncidence, les maîtres du monde physique et virtuel viennent tous de la même contrée. Pour le dire simplement, ces deux mondes ont les mêmes maitres. Ce sont les deux grandes superpuissances politiques et économiques de l'heure qui les produisent. En tête, naturellement, la superpuissance américaine, avec ses GAFAM (Google, Apple, Facebook, Amazon et Microsoft) et NATU (Netflix, Airbnb, Tesla et Uber), secondée par la puissance chinoise, avec BATX (Baidu, Alibaba, Tencent et Xiaomi). Cette technologie cybernétique a rendu possible la collecte des données sur les crimes et les conflits, améliorant l'efficacité de l'alerte précoce et une réponse appropriée.

Au niveau de l'échelle des valeurs, le cyberespace numérique s'est positionné comme la quatrième dimension géopolitique, avec des changements majeurs qui imposent une adaptation rapide, permettant de garder le cap sur l'évolution de la société humaine. Il ne faut, d'ailleurs pas perdre de vue que le cyberespace est à la fois un enjeu de rivalités de pouvoir entre les acteurs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques **(Pr Alice NGA MINKALA, Dr BABA WAME et M. Prosper DJOURSOURBO PAGOU**).

Sortant du cadre classique de l'information, la médiacratie cybernétique présente plusieurs facettes complexes qui la rendent incontournable et lui donne le visage d'une hydre.

B- L'ESSOR DE L'HYDRE CYBERMEDIATIQUE

L'avènement de l'internet ubiquitaire ainsi que de l'égalitarisme fanatique dont il procède, sont producteurs de profonds dysfonctionnements sociaux majeurs, catalysés par la capacité exponentielle qu'ont les médias sociaux de

mobiliser des opinions et ressources parfois contradictoires. Dans cette nouvelle société néolibérale, caractérisée par le doute et sur laquelle l'Etat a perdu le contrôle **(Pr Nadine MACHIKOU)**, la médiacratie cybernétique tend à prendre la relève de façon anarchique. A travers l'établissement d'une cyberdiplomatie, on note la formation des alliances numériques constituant un indicateur de la puissance dans les relations internationales. En effet, la maitrise de l'internet constitue un enjeu de puissance complètement étranger à l'ordre westphalien et post westphalien **(Pr Jean NJOYA)**. Cet ordre, où le territoire a été et est la seule variable de codification des relations internationales, se mue insensiblement en un lieu de «*turbulences*» dans desquelles les flux transnationaux s'opèrent.

C'est désormais dans ces flux transnationaux que se meut l'essentiel de la vie sociale, économique et culturelle et où se bâtissent de nouveaux imaginaires territoriaux transgressifs. Dès lors, l'on ne peut parler de territoire aujourd'hui sans évoquer la problématique la plus débattue de la dernière décennie, à savoir **«la fin des territoires»**. Celle-ci tient aux bouleversements spectaculaires qui marquent la scène internationale et est essentiellement liée à la révolution des communications, qui a ouvert de nouvelles routes mondiales n'ayant plus de base étatique.

Dans cette perspective, le cyberespace constitue véritablement un terrain d'affrontement au sens propre et figuré du mot, qui met en scène des groupes d'acteurs savamment organisés pour des fins de déstabilisation. Dans son viseur, il tient particulièrement en vue les forces de défense et de sécurité, boucliers de la société **(Lieutenant-Colonel Brice MIMBOLO)**. Ainsi, la cyberguerre, devenue fondamentale dans les relations internationales, est un outil de guerre d'information et de la propagande qui a contraint les Etats à développer des stratégies de cyberdéfense afin de réduire ces risques qu'atténue la gouvernance du cyberespace. C'est pourquoi, la défense, à travers la cybersécurité, est devenue l'un des enjeux politiques et économiques **(Pr Désiré AVOM)**.

Si la médiacratie cybernétique est une arme de construction massive, elle apparaît également, et de plus en plus, comme un outil de destruction et de déstabilisation massive. En effet, l'irruption des réseaux sociaux, plates-formes d'échanges entre les personnes, a suscité des appétits *«criminels»* au sein de la communauté humaine. Aussi, note-t-on des exactions enregistrées, notamment

par les actions de l'ingénierie sociale **(Mme Françoise EKOLLO)**. Il en est ainsi des «*fake news*», de «*phishing*», etc. Dans le domaine de la cybercriminalité, les conséquences sont perceptibles, notamment, sur le plan économique et social. Les chiffres sur des arnaques, des fraudes dans les services de la téléphonie mobile démontrent à profusion de la gravité de la situation (ces données chiffrées sont estimées à environ 4 milliards de FCFA depuis 2010 au Cameroun).

Ainsi, s'il est incontestable que la généralisation, voire la démocratisation des technologies de l'information et de la communication est une opportunité non seulement pour les institutions publiques ou privées, mais aussi pour les individus des pays en développement comme le Cameroun, elle constitue, en même temps, l'une des plus grosses menaces qui pèsent sur ces entités, au regard de l'usage qu'en font certains individus, malveillants, au demeurant. Le Cameroun a fini par prendre conscience de ce danger que représente cet usage malveillant qu'est la cybercriminalité, et a mis en œuvre des mécanismes textuels, institutionnels et, dans une moindre mesure, infrastructurels, pour y faire face. Toutefois, ce dispositif a besoin d'un soutien extérieur, au-delà du fait qu'il doit, sans cesse, s'ajuster et se réinventer.

Les acteurs cybercriminels ne sont pas les seuls qui s'écartent de l'éthique. En effet, ceux qui sont légalement reconnus dans et par le cyberespace, ne sont pas exempts de tout reproche. Les GAFAM, BATU, BATX, notamment, s'illustrent par une avidité obsessionnelle et inquiétante pour le monopole du secteur. Ainsi, lorsqu'ils ne peuvent pas s'inventer, ils n'hésitent pas à déployer toutes les stratégies prédatrices pour absorber les nouvelles «*Start up*» potentiellement très porteuses, à coups de milliards de dollars. De façon plus pernicieuse, ces géants du numérique se nourrissent des données d'utilisateurs acquises gratuitement, mais revendues à prix d'or aux prestataires publicitaires. Or, ces données ne servent pas uniquement des fins lucratives. Par des milliers de données qu'ils détiennent sur leurs utilisateurs, ils font une intrusion fort nuisible dans leur vie privée, au point de les connaitre, peut être mieux qu'eux-mêmes. Une telle intrusion pose incontestablement le problème du respect du droit à l'intimité et du droit à la vie à l'ère du numérique à outrance. En contrôlant ainsi les individus, ils ont en réalité une main mise sur leurs Etats, notamment sur leurs choix technologiques et politiques **(Dr BABA WAME)**. D'où **l'intérêt pour les Etats, notamment africains, de construire leur indépendance numérique**, afin de sortir de la colonisation numérique, un

ordre d'asservissement et d'avilissement.

Au regard de cette utilisation à des fins multiples de la médiacratie cybernétique, force est de constater que celle-ci finit par échapper au contrôle des Etats qui, de façon réactive, tentent de se donner plus de moyens pour l'intégrer désormais dans son système. Ceci participe de la nécessaire maitrise par ces Etats de ce chamboulement cybermédiatique.

II- LA NECESSAIRE MAITRISE DU CHAMBOULEMENT CYBERMEDIATIQUE

La gestion sereine de «*l'ouragan cybernétique*» impose aux Etats, ainsi qu'aux acteurs privés, de se réinventer en se saisissant de cette puissance médiatique, qu'il importe d'apprivoiser et d'encadrer. Ceci passe d'une part, par **le retour à un ordre normal, garant des libertés (A), et, d'autre part, par la prise en main de l'ordre cybermédiatique, facteur de développement humain durable (B)**.

A- LE RETOUR A UN ORDRE NORMAL, GARANT DES LIBERTES

Compte tenu de la transformation cybernétique, il revient à l'Etat de reconstruire son image, sans cesse ternie par les médias **(Pr Nadine MACHIKOU)**. Une sonnette d'alarme a été lancée sur l'urgence et la nécessité pour les États d'instaurer un ordre juridique numérique ainsi qu'une mutualisation, une coopération, une harmonisation et une coordination des divers mécanismes étatiques de lutte contre la propagation de comportements à risque sur la sphère cybernétique **(Pr Alain KENMOGNE)**. Le vide juridique constaté dans le cadre de l'encadrement, mais surtout de la répression de certains actes cybercriminels, tels que l'usurpation d'identité, la vengeance pornographique, les *fake news*, ne facilite pas une réponse adéquate et adaptée à la proportion de l'acte posé **(CD Thierry MEDOU)**. Pour ce faire, le prolongement juridique de l'encadrement international technique du cyberespace doit s'accentuer et provoquer une internalisation des instruments juridiques internationaux déjà existants.

Il revient donc à l'Etat de penser une gamme de mesures pour panser le mal cybernétique, devenu une menace à la sécurité. La mise sur pied d'une coopération juridique internationale peut être un moyen pertinent pour enrayer les effets pervers de ce phénomène. Face à cette ambivalence du cyberespace, il importe de consolider la gouvernance numérique pour la cybersécurité et contre la cybercriminalité, afin d'assurer une gestion effective des risques et cybermenaces, d'où l'urgence de développer un programme de cyber résilience.

La capacitation des pays à la maitrise de l'espace cybernétique devient donc un indicateur de la puissance et de développement. Les Etats doivent être proactifs, afin de mieux anticiper sur le risque cybernétique. Au Cameroun, par exemple, la législation portant sur l'encadrement de l'accès au cyberespace est articulée autour de deux pôles: la consécration d'un droit d'accès de toutes les personnes au cyberespace et le contrôle par l'Etat de tout le processus d'accès y relatif **(Pr Etienne KENFACK)**. Il est évident que les réponses étatiques, essentiellement unilatérales, apportées n'endiguent pas la cybercriminalité. Elles doivent compléter par des initiatives et approches globalisantes au niveau sous-régional, régional et universel.

Au niveau régional, la vulnérabilité persistante de l'Afrique, malgré les avancées considérables dans ce domaine est palpable, tout comme la faiblesse des investissements nationaux en matière d'infrastructure à l'origine du coût élevé de l'accès à internet. Ce qui fait de ce continent, un marginal dans le marché capital du cyberespace. Au Cameroun, le Gouvernement a intensifié timidement la sécurisation de son cyberespace. A cette riposte, qui porte des fruits, il est désormais impératif de renforcer les capacités institutionnelles, normatives et humaines des acteurs et de mettre en œuvre la Convention de Malabo **(CD MEDOU Thierry)**.

Pour qu'un pays moins bien doté en termes de technologies de contrôle des flux numériques, tel que le Cameroun, s'impose indubitablement, il est nécessaire qu'il repense l'espace public numérisé dans le sens de sa focalisation sur les questions plus sociales et moins politiques **(Mme Pierrette EVINA)**. Pour faire face aux attaques, quatre approches doivent être déployées de façon simultanée, pour garantir une meilleure efficacité: la **dissuasion**, la **prévention**, la **détection** et la **réaction**. Il importe, par ailleurs, d'opérer une distinction entre cybersécurité et cyberdéfense (la première notion relève, en effet, du domaine civil, avec une posture essentiellement défensive, tandis que

la seconde relève du domaine militaire, avec une posture résolument offensive). Afin de garantir les actions de riposte des Etats, les nouveaux maîtres du monde, qu'incarnent les principales multinationales contrôlant le marché du numérique (les GAFAM, BATU, BATX), s'imposent de fait comme leurs principaux interlocuteurs dans la perspective de l'assainissement du cyberespace et de la lutte contre les cybermenaces.

Au demeurant, **la liberté, la vraie, celle de la personne humaine qui s'achève là où commence celle de l'autre, en dépend**. Ainsi, tous les acteurs privés et publics du cyberespace devraient travailler de concert, en étroite synergie de manière à repousser l'**«Arsenalisation»** de l'espace cybernétique par les groupes terroristes et sécessionnistes **(Lieutenant-Colonel Brice MIMBOLO)**. Les pays africains, ainsi que les institutions de sécurité, à l'instar de l'EIFORCES, doivent absolument exploiter l'opportunité cybernétique, afin de limiter les risques inhérents à l'émergence des dérives liées à l'avènement et l'essor de cette forme technologique, afin de contribuer à la consolidation de la paix et de la stabilité **(Nii ODARTEY)**. Il s'agit donc d'une prise en main de l'ordre cybermédiatique, facteur de développement humain durable.

B- LA PRISE EN MAIN DE L'ORDRE CYBERMEDIATIQUE, FACTEUR DE DEVELOPPEMENT HUMAIN DURABLE

Le cyberespace a rendu les flux financiers productifs et fluides, consacrant la **nanoseconde** comme l'unité de temps de déclenchement des ordres de bourse. En tant que sources d'externalité, d'incitation et d'opportunités, le cyberespace, grâce au marché numérique, offre de nouvelles aubaines commerciales dans les pays émergents, en favorisant l'interconnexion des marchés financiers.

Au demeurant, l'interconnexion des réseaux et systèmes du numérique induit leur interdépendance et accroit leur perméabilité par des cybercriminels. Ce qui rend impératif la coordination des réponses cybersécuritaires pro-actives, actives et réactives, tant à l'échelle nationale (à travers la recherche, l'éducation et le dialogue avec tous les acteurs du cyberespace), qu'internationale, par la consolidation du cyberdroit **(Pr Justine DIFFO TCHUNKAM)**.

L'utilisation stratégique de l'économie des médias et des nouveaux médias dans la préservation de la souveraineté des Etats africains, notamment de la souveraineté économique, doit être prise en compte par les pouvoirs publics. La mobilisation stratégique des médias, comme facteurs de puissance sur le plan intérieur en Afrique est aussi un intérêt à la portée des Etats africains **(Pr Guy MVELLE MINFENDA)**. Dans ce théâtre compétitif, le secteur des médias et de la communication apparait comme un outil déterminant que mobilisent les acteurs stratégiques dans la perspective d'assurer la réussite de leurs stratégies dans des marchés précis à travers les principes de «*local contain*».

La cryptographie n'est pas en reste. Sa base étant la tokenisation, elle apporte les fonctions de confiance qui permettent au cyberespace numérique de bénéficier des propriétés telles que l'authenticité, la non-répudiation, l'intégrité la transparence et ou la confidentialité. Il apert donc que la cryptomonnaie, qui sied mieux à l'espace numérique, présente non seulement des avantages, mais également des risques dont les facteurs pourraient être atténués **(Pr Georges BELL BITJOKA)**.

La «démocratisation» de l'information, à travers le canal digital, pose le triple problème du droit de savoir du public, du devoir de réserve et de la nécessité du secret d'État. Le contrôle de l'information est un préalable de sécurité nationale. A ce sujet, la riposte communicationnelle de l'armée est vitale pour sa propre survie et celle de la société entière. Elle doit, de ce fait, prendre le dessus sur la menace. Sa raison d'être consiste alors à susciter l'adhésion, à promouvoir son image de marque, à promouvoir son l'influence. Il est donc nécessaire qu'on passe d'une Communication de Défense et de Sécurité, centrée sur le pouvoir et les décisions de l'Etat, vers une Communication sociale de Défense et de Sécurité, plus accommodante pour les populations **(CV Cyrille Serge ATONFACK NGUEMO)**.

CONCLUSION

Que dire en conclusion ? Des communications riches, des échanges courtois et porteurs ont ponctué ce Colloque international. Incontestablement, les résultats attendus ont été atteints. La preuve en les recommandations qui en ont résultées.

Ces recommandations sont adressées à trois catégories d'acteurs: les **Etats**, les **partenaires internationaux** et la **société civile**.

1-Pour ce qui est des Etats, en tant que régulateur de tout le secteur médiatique, ils sont invités à:

- renforcer la sensibilisation des utilisateurs, à travers l'adoption de stratégies de communication adaptées, en mettant l'accent sur les cibles privilégiées que sont les jeunes et en renforçant, en améliorant la visibilité numérique des acteurs sécuritaires dans la perspective de la lutte contre la propagande et les discours haineux;
- favoriser le développement des plateformes locales, afin de garantir une meilleure traçabilité des données numériques et la sécurisation des données privées et de celles stratégiques;
- renforcer la formation continue des personnels du secteur public en général et ceux des domaines liés de la défense et de la sécurité, en particulier, en vue de leur mise à niveau en matière de manipulation responsable, de sécurisation des contenus digitaux et surtout de communication digitale;
- mettre en œuvre au niveau national des centres agréés de cyberdéfense. A ce titre, une autorité nationale de lutte contre la cybercriminalité pourrait être conçue et opérationnalisée;
- articuler des politiques publiques destinées à encourager les investissements dans la recherche-développement en matière de TIC;
- concevoir un véritable cadre juridique en matière de prévention et de répression de la cybercriminalité, pour favoriser de bonnes pratiques permettant de lutter contre ce phénomène;
- renforcer le partenariat public-privé, en vue de structurer la coproduction d'un discours sécuritaire plus inclusif, affranchi de l'étiquette monopolistique de l'Etat;
- favoriser la mobilisation des expertises et des outils suggérés par les acteurs du secteur privé pour l'amélioration des usages, des stratégies et des politiques en adéquation avec la nouvelle donne digitale au sein des administrations publiques.

2- Pour ce qui est des partenaires internationaux, ils sont invités à:

- renforcer la coopération avec les Etats en vue de faciliter le partage des informations pertinentes sur les cybermenaces et les consommateurs potentiellement dangereux;
- mutualiser, à l'échelle africaine, des savoirs technologiques, des moyens et des ressources humaines dans l'optique de renforcer l'appropriation par les différentes catégories de consommateurs africains de produits numériques et des innovations en la matière;
- multiplier les efforts diplomatiques pour obtenir partout en Afrique et au-delà, des accords de coopération judiciaire et policière dans le domaine de la lutte contre la cybercriminalité;
- travailler de concert à la coordination de la réponse cybersécuritaire à travers un effort d'harmonisation des dispositifs normatifs et des mécanismes de répression de la cybercriminalité et de la cyberdélinquance.

3-Enfin, pour ce qui est de la société civile, elle est invitée à:

- contribuer à l'effort collectif de sensibilisation des populations en général, et de la jeunesse en particulier, impulsé par les Etats, dans l'optique de favoriser l'usage responsable des média sociaux;
- encourager la création de plateformes citoyennes, à l'effet de proposer des modules d'éducation citoyenne aux TIC;
- développer une culture du référencement et de la dénonciation de contenus et/ou d'utilisateurs dangereux afin de contrecarrer les discours haineux et autres formes d'activités illicites menées à travers Internet et les média sociaux.

Le colloque s'est achevé avec le mot de clôture du Secrétaire d'Etat à la Défense, chargé de la Gendarmerie Nationale, Représentant le Ministre Délégué à la Présidence, chargé de la Défense, Président du Conseil d'Administration de l'EIFORCES.

Je vous remercie pour votre attention soutenue.

Yaoundé, le 29 avril 2022

ALLOCUTION DE CLOTURE

Monsieur Galax Landry ETOGA
Secrétaire d'Etat auprès du Ministre de la Défense chargé de la Gendarmerie Nationale
Représentant le Ministre Délégué à la Présidence chargé de la Défense
Président du Conseil d'Administration de l›EIFORCES

Nous voici parvenus à l'issue des travaux du Colloque International sur le thème: ***«MEDIACRATIE CYBERNETIQUE ET MENACES SECURITAIRES: ENJEUX, DEFIS ET REPONSES A L'ERE DE LA DIGITALISATION»,*** organisé par l'Ecole Internationale des Forces de Sécurité (EIFORCES) à travers son Centre de Recherche et de Documentation.

Je tiens à réitérer ma gratitude et ma reconnaissance à Monsieur le Ministre Délégué à la Présidence chargé de la Défense, Président du Conseil d'Administration de l'EIFORCES, pour toute la confiance accordée à notre institution, ainsi que pour les diligences entreprises afin de faciliter la tenue et la réussite de cette activité.

Chers participants, intervenants et modérateurs, permettez-moi de vous remercier, pour le dévouement et l'abnégation dont vous avez fait montre durant ces deux jours d'échanges riches et fructueux.

Mes remerciements vont aussi à l'endroit des auditeurs de la 8ème promotion du Brevet d'Etudes Supérieures de Sécurité, dont la présence et la participation, à bien des égards, illustrent de la pertinence d'une synergie axée sur le renforcement de la formation à travers la recherche. A travers vos contributions, on a pu davantage se rendre compte du caractère global et international de la médiacratie cybernétique et l'urgence d'une vision

commune dans la recherche des solutions pour mieux l'adresser.

La cybercriminalité, la cybersécurité, la médiacratie, nous en parlons, depuis quelques années déjà ! L'urgence est à l'action et à la mutualisation des efforts. Tous les acteurs devraient désormais parler d'une seule voix. Il y va de la sécurité, de la stabilité et du développement de nos Etats. En tant qu'outil de politique publique de l'Etat et de la Communauté Internationale en matière de sécurité globale, l'EIFORCES ne saurait rester à l'écart de la réflexion.

Vivement, que les structures décisionnelles et opérationnelles en charge de ces questions passent à l'action pour que la dignité, l'intégrité, la sécurité des personnes physiques et morales soient davantage renforcées aussi bien dans l'espace virtuel que dans l'espace physique. Ce faisant, en tant que fer de lance de la Nation, l'éducation et la sensibilisation à un usage plus responsable de ces outils technologiques ne devraient-elles pas s'accentuer auprès des plus jeunes ?

*Plus que par le passé, on assiste à la faveur de la Mondialisation à des reconfigurations et mutations de l'espace virtuel où discours haineux, violence verbale, fake news et autres cyberattaques relèvent désormais de l'ordre de la banalité. C'est conscient de cet enjeu, défi actuel et complexe, et fidèle à sa tradition en matière de formation et de recherche dans les domaines de la sécurité et des opérations de paix que l'Ecole Internationale des Forces de Sécurité (EIFORCES), a adressé la problématique de la "*médiacratie cybernétique et menaces sécuritaires : enjeux, défis et réponses à l'ère de la digitalisation* ". Réunis du 28 au 29 avril 2022, au Palais des Congrès de Yaoundé, des acteurs privés et publics, du champ universitaire, de la défense et de la sécurité, des technologies de l'information et de la communication, de l'informatique, ont analysé, réfuté et proposé des solutions face à une problématique qui affecte tant la sûreté que la sécurité des personnes physiques et morales, ainsi que leurs biens . Les recommandations de ce Colloque International, devenu un traditionnel brainstorming national et international de l'EIFORCES, ont mis l'accent, pour l'essentiel, à un usage vertueux et responsable de l'espace virtuel et des technologies de l'information et de la communication, en plaçant l'humain au centre de ces changements transformationnels./-*

www.eiforces.com

Revue scientifique
éditée par l'EIFORCES