EXPERTISE ET ACTION PUBLIQUE DE LUTTE CONTRE LA CYBERCRIMINALITE LE LONG DE « LA CEINTURE ET LA ROUTE » AU CAMEROUN

Alain-Patrick LOUMOU MONDOLEBA
Université de Douala, Cameroun
loumoupatrick16@gmail.com

Résumé

Cet article tente de montrer l'intérêt du recours aux experts dans l'action publique de lutte contre la cybercriminalité le long de l'initiative chinoise « la ceinture et la route » au Cameroun. Les connexions et les dynamiques d'interdépendances multiformes que la Chine entend créer avec ses partenaires, à travers cette initiative, ne se limitent pas à leur seule dimension physique ; elles intègrent également leur dimension virtuelle ou numérique. Toutefois, le risque pour que cette ambition se heurte au fléau de la cybercriminalité est quasi indéniable. Considérée aujourd'hui comme la troisième plus grande menace des grandes puissances, après les armes chimiques, bactériologiques et nucléaires (Colin, 2000), la cybercriminalité n'a cessé de prendre, au cours de ces dernières années, des proportions considérables aussi bien en Chine qu'au Cameroun. De ce fait, cette réflexion informe sur la coopération sino-camerounaise autour des politiques publiques de lutte contre la cybercriminalité dont la complexité et la technicité forcent la collaboration et la co-production pour l'atteinte des résultats efficaces. Quel est l'intérêt du recours aux experts ? Comment la coopération experte entre la Chine et le Cameroun peut-elle concourir à l'efficacité de l'action publique de lutte contre la cybercriminalité le long de l'initiative « la ceinture et la route » ? L'étude fait le pari théorique et méthodologique de mobiliser l'analyse cognitive dont la pertinence est de saisir en pratique les idées, les connaissances, les valeurs et les interprétations des experts impliqués dans la production de l'action publique de lutte contre la cybercriminalité le long de l'initiative chinoise « la ceinture et la route » au Cameroun. De plus, elle mobilise une grille empirique tournée vers la recherche documentaire et les entretiens.

Mots-clés *: Expertise, cybercriminalité, Cameroun, Chine, « Ceinture et la route ».*

Summary

This article tries to show the interest the use of experts in public action to fight against cybercrime along the Chinese initiative "the belt and the road" In Cameroon. The connections and dynamics of multiform interdependence that China intends to create with its partners through this initiative are not limited to their physical dimension alone, they also include their virtual or digital dimension. However, the risk that this ambition will come up against the scourge of cybercrime is almost undeniable. Considered today as the third greatest threat to the great powers, after chemical, bacteriological and nuclear weapons (Colin, 2000), cybercrime has continued to take on considerable proportions in recent years, both in China than in Cameroon. Therefore, this reflection intends to inform on the Sino-Cameroonian cooperation around

public policies to fight against cybercrime whose complexity and technicality force collaboration and co-production to achieve effective results. What is the benefit of using experts? How can expert cooperation between China and Cameroon contribute to the effectiveness of public action to combat cybercrime along the "Belt and Road" initiative? The study makes the theoretical and methodological bet to mobilize cognitive analysis, the relevance of which is to grasp in practice the ideas, knowledge, values and interpretations of the experts involved in the production of public action in the fight against cybercrime. In addition, it mobilizes an empirical grid oriented towards documentary research and interviews.

Keywords: *Expertise, cybercrime, Cameroun, China, "Belt and Road".*

Introduction

L'une des spécificités de la mondialisation est l'extension de « la société du savoir » (Bindé, 2005 ; Padioleau, 2001) qu'elle provoque, et qui traduit l'idée d'une société marquée par le développement accéléré des technologies de l'information et de la communication (TIC) et l'usage abondant et varié de l'outil Internet. Toutefois, les TIC constituent autant un outil d'épanouissement (économique, social et culturel) qu'un risque pour la société moderne. D'ailleurs, selon Ulrich Beck (2001), le développement des TIC est corrélé à « la production sociale du risque » (p. 36). Cette réflexion met donc un point d'honneur sur les risques de cybercriminalité auxquels l'initiative « la ceinture et la route » pourrait être confrontée en Afrique francophone et s'emploie à montrer la nécessité qu'il y a d'initier des dynamiques de coopération experte entre la Chine et les pays de cette partie du continent pour mieux adresser la question. En effet, la cybercriminalité a pris une part croissante et est désormais considérée comme l'un des risques sécuritaires majeurs de l'époque actuelle. Ainsi que le souligne Rose Colin, elle constitue « la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques et nucléaires » (Colin, 2000 : 12).

Dans une perspective définitionnelle, la cybercriminalité est souvent assimilée à un « ennemi désétatisé et déterritorialisé » (Beck, 2009), ceci en raison du fait qu'elle n'est pas une menace physique, mais virtuelle. Littéralement, la cybercriminalité englobe les infractions, les crimes et toutes les actions illégales commises dans le monde numérique, notamment sur Internet. Dans le cadre de cette étude, elle s'entend comme « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent » et dans une acception plus large « tout fait illégal

commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique » (ONU, 2000 : 1).

D'après une étude menée par l'éditeur d'antivirus McAfee en 2017, la cybercriminalité a engendré un préjudice estimé à 1000 milliards de dollars en 2008, équivalant à environ 1,64% du PIB mondial. Aujourd'hui, la cybercriminalité coûte au monde entier près de 600 milliards de dollars, soit 0,8 % du PNB mondial, selon le nouveau rapport publié par le *Center for Strategic and International Studies* (CSIS) et McAfee. Cette montée en puissance de la cybercriminalité dans le monde est due au fait qu'en effet, au cours de ces dernières décennies, on assiste à l'avènement d'une « société virtuelle » où tout semble se numériser, et où tout est une reproduction et un prolongement de la vie réelle. Il faut dire qu'Internet et les technologies affectent pratiquement toutes les sphères (économique, sociétale et culturelle) de la vie moderne et façonnent notre quotidien (Unicef, 2017). Se situant dans cette perspective, Marshall McLuhan (1977) souligne que les technologies sont le prolongement de nos organes physiques et de notre système nerveux, dont l'une des ambitions est d'accroître la force et la rapidité. Il fait observer que le téléphone est un prolongement de la bouche et des oreilles voire de l'ouïe, la télévision un prolongement des yeux et de la vue, la voiture ou les roues un prolongement des pieds, etc. Si Internet a été pensé comme un outil d'optimisation de leurs performances et de leur utilité, il n'en demeure pas moins vrai que son utilisation déviante entraîne diverses formes de criminalité : extorsions de fonds ; fraudes liées à la carte de crédit ; fraudes commerciales ; abus de confiance et escroqueries diverses ; usurpations d'identités ; détournements de mineurs ; hameçonnage ; rançongiciel (ou « *ransomware* » en anglais) ; attaque en déni de service ; la contrefaçon numérique ; cyberterrorisme, etc.

Plus d'un million de personnes dans le monde sont victimes de la cybercriminalité par jour (Matignon, 2012). Malgré que l'Afrique soit le continent qui a la connectivité Internet la plus faible du monde, avec 28 % d'utilisateurs Internet en 2019, contre 83 % de la population en Europe (Interpol, 2020), les groupes criminels organisés utilisent les outils en ligne pour un large éventail d'activités illicites. Le nombre de cyberattaques enregistrés sur le continent africain au cours de ces dernières années n'a cessé d'augmenter exponentiellement. D'après les statistiques fournies par le cabinet Shadow Market (2011), 12 pays arrivent en tête au classement des parcs informatiques les plus infectés

en Afrique : Libye (98%), Zimbabwe (92%), Algérie (84%), Cameroun (83%), Nigeria (82%), Zambie (82%), Côte d'Ivoire (81%), Kenya (78%), Sénégal (78%), Tunisie (74%), Maroc (66%) et Ile Maurice (57%). Selon le rapport d'Interpol de 2019, un des facteurs clés de cette augmentation d'actes criminels sur Internet en Afrique est que de nombreux pays ne disposent pas de politiques et de stratégies globales réelles de lutte contre la cybercriminalité. Bien que l'Union africaine (UA) ait adopté sa Convention sur la cybersécurité et la protection des données à caractère personnel en 2014, seuls 14 de ses 55 pays membres l'ont signée jusqu'en août 2020. En Chine, la cybercriminalité bat son plein. Avec plus de 670 millions d'internautes, la Chine constitue l'un des pays au monde où les hackers disposent du plus grand vivier de cibles potentielles (Fillipone, 2017). Elle est « le pays le plus connecté du monde » (Lecalot, 2021).

La technicité à laquelle sont confrontés les décideurs publics dans la production des politiques publiques cybersécuritaires affecte la manière dont se conçoivent leurs liens avec les experts (Jacob et al, 2005). Au fond, la sociologie du risque et la sociologie de l'expertise sont indissociables (Beck, *op.cit.*). En s'ancrant dans l'analyse cognitive et la théorie de l'apprentissage, cette étude postule en faveur d'une action publique anti-cybercriminalité qui repose sur l'indissociabilité entre pensée et action, entre savoirs et décisions le long de « la ceinture et la route ». Si les cas de cybercriminalité n'ont cessé de se multiplier en Afrique francophone et ailleurs, c'est sans doute parce que les Etats ont pendant longtemps arboré la figure de « l'Etat à tâtons » (Cantelli, 2007) dans son appréhension, s'illustrant dans son déploiement quotidien, par « débrouillardise » (Lindblom, 1979) et par tâtonnement. Les agents d'Etat n'étant pas toujours en possession des capacités et des moyens cognitifs nécessaires pour produire des politiques publiques efficaces de lutte contre la cybercriminalité, les Etats entreprennent de mettre sur pied un processus de couplage (Zittoun, 2003) et d'ajustements mutuels (Massardier, 2003). De ce fait, l'action publique de lutte contre la cybercriminalité le long de la « ceinture et la route » doit s'inscrire dans le schéma de la co-production entre les décideurs politiques et les experts.

Comment la coopération experte peut-elle contribuer à rendre l'action publique de lutte contre la cybercriminalité le long de l'initiative chinoise « la ceinture et la route » au Cameroun ? Telle est la question à laquelle cette étude entend trouver des réponses. Elle défend l'hypothèse selon laquelle la coopération experte constitue, non seulement un cadre de

rationalisation de l'action publique de lutte contre la cybercriminalité, mais aussi une modalité de simplification du risque par le partage d'expériences. Dans cet élan, la réflexion s'efforce de considérer l'action publique de lutte contre la cybercriminalité comme une politique publique du risque, c'est-à-dire un ensemble de moyens de riposte contre le risque que constitue la cybercriminalité. Risque pour la sécurité des populations, risque pour le bon fonctionnement des institutions publiques et des entreprises privées, risque pour l'économie du pays, etc. L'étude s'ordonne autour de deux grands axes : d'abord, s'emploie-t-elle à analyser l'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route » comme une « situation d'expertise » (1) ; ensuite, entend-elle de montrer comment la collaboration experte peut s'avérer une modalité de rationalisation de l'action publique anti-cybercriminalité le long de « la ceinture et la route » (2).

1. L'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route » comme situation d'expertise

Comme cela a été précédemment indiqué, l'initiative « la ceinture et la route » est un projet qui accorde une place importante à l'aspect numérique, mieux cybernétique des dynamiques d'interdépendances économiques, sociopolitiques et culturelles (Nantulya, 2019). « La route de la soie numérique » qui fait partie de ses points structurants, et dont l'ambition est de permettre à la Chine d'accroître ses parts de marché et d'acquérir une position dominante dans les économies émergentes ainsi que sur les marchés plus développés, est un projet porté en grande partie par des entreprises technologiques chinoises (Tybring-Gjedde, 2020). Evidemment, cela s'explique par la position décisive que la Chine occupe sur l'échiquier numérique mondial. Le programme « China Standards 2035 » reflète clairement sa volonté de se poser en référence mondiale dans le domaine des technologies émergentes, notamment la 5G, l'intelligence artificielle et l'internet des objets (Dekker et al., 2020). Les œuvres numériques que la Chine entend réaliser à travers l'initiative « la ceinture et la route » sont entre autres : la construction de réseaux de télécommunications, le commerce électronique, les nanotechnologies, l'informatique quantique et la mise en place d'un système complet de satellites multifonctionnels. Bien plus, la Chine envisage améliorer, à travers « la route de la soie numérique » se propose, la connectivité

régionale et internationale dans les domaines des infrastructures, du commerce, de la finance et du « cœur des gens » (Dekker et al., 2020).
Tous ces progrès sont susceptibles d'engendrer de nouvelles fragilités et vulnérabilités propices aux menaces ou aux risques de cybercriminalité le long de l'initiative « la ceinture et la route ». L'espace cybernétique est devenu est un espace de désinformation, d'intimidation, d'appel à la haine, aux meurtres, à la violence (Aby, 2020). L'Etat, le gouvernement, les forces de l'ordre et de sécurité, les entreprises et les populations ont besoin de cerner toute sa complexité (Haddad, 2017) et la matérialité de ses enjeux, pour mieux valoriser et veiller à la préservation de leurs intérêts. Cependant, il est un constat que les politiques publiques de lutte contre la cybercriminalité sont longtemps/jusqu'ici restées dominées par la perspective normativiste et institutionnelle (Delerue & Aude, 2018 : 61-70), alors qu'elles nécessitent d'être pensées en termes de rationalité scientifique et technique. Et cela implique de recourir aux experts.
L'expert doit être perçu comme une personne qui dispose d'une gamme de compétences et d'expérience et qui est sollicitée par une autorité publique pour l'aider à résoudre un problème donné, et/ou à prendre une décision. C'est la « situation d'expertise » (Cresal, 1985) qui donne vie au statut d'expert. Celui-ci se démarque quelque peu de la figure de l'intellectuel (Zola, 1898) qui, lui se caractérise par sa liberté d'esprit et de critique et se veut fidèle à un ensemble de valeurs (neutralité, intégrité, objectivité) (Weber, 1919). L'expert quant à lui est mandaté ; il agit suivant un cahier de charges bien défini et est parfois est soumis au décisionnisme de l'autorité politique par qui il a été mandaté. Toutefois, il est important de ne pas opposer les deux ici. Autant l'expert produit une expertise interne, autant l'intellectuel produit une expertise externe, toutes utiles à l'action de lutte contre la cybercriminalité. Au-delà du fait qu'elle soit utile à la société, l'expertise de l'intellectuel contribue au progrès de la science. Elle est une production de conviction et de « vocation » (*Ibid.*).

1.1. Le recours aux experts comme registre privilégié dans les processus de production de l'action publique de réduction du risque

Le recours aux experts se présente comme une nécessite dans les processus d'apprentissage des agents d'Etat. L'expertise se veut non seulement une aide à la décision, mais aussi une modalité de réduction de

l'incertitude et de simplification de la technicité du problème de la cybercriminalité. L'idée que l'on veuille véhiculer à travers le concept d'apprentissage est qu'il est nécessaire d'introduire l'incertitude et la mobilisation des savoirs pour comprendre la conduite des politiques publiques dans les sociétés contemporaines (De Maillard, 2010). Les processus d'apprentissage sont une activité dont le but est d'atteindre plus efficacement les objectifs d'une politique (Sabatier & Schlager, 2000, pp. 209-234). Il peut s'agir, soit de faciliter l'acquisition d'une meilleure compréhension de la gravité d'un problème, de ses causes, des bénéfices et des coûts des solutions alternatives, soit d'identifier les ressources cruciales et leur origine, d'identifier des menaces pesant sur le pouvoir de l'organisation ainsi que les stratégies visant à accroître ce pouvoir (Ibid). L'affirmation des experts dans les processus d'apprentissage des stratégies et de l'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route » au Cameroun56+ peut s'opérer par le biais de nombreuses formations qu'ils offrent aux personnels des différentes institutions en charge de l'élaboration et de la mise en œuvre de la politique de lutte contre la cybercriminalité, et aussi par le biais des conférences et colloques organisées par ces institutions et auxquelles ils sont conviés.

Autrement dit, il s'agit de doter les différents acteurs des connaissances techniques contre ces pratiques malsaines pour une bonne maîtrise des formes de cybercriminalité. On assiste à la prégnance du besoin de formation. Ce besoin s'explique notamment par la technicité de la cybercriminalité. Au Cameroun par exemple, le gouvernement a parfois eu recours aux partenaires experts d'INTERPOL et autres institutions internationales pour affiner les méthodes de lutte contre les cybers attaques au Cameroun. Présentement, le Cameroun collabore avec l'Organisation du Commonwealth pour les télécommunications (CTO) dans ce sens. Une collaboration qui, selon la ministre des postes et télécommunication va permettre à l'État du Cameroun de bénéficier des expériences des membres de le CTO les plus avertis en la matière. On part de l'idée que les acteurs en charge d'élaborer et d'implémenter la politique de lutte contre la cybercriminalité doivent suivre le rythme des évolutions technologiques. Ils doivent disposer de l'expertise et des compétences nécessaires pour gérer la criminalité numérique, qui ne cesse d'évoluer, au niveau national, régional et international.

1.2- Les modalités de participation possible des experts à la production de l'action publique contre la cybercriminalité le long de « la route et la ceinture » au Cameroun

Les colloques, conseils et les consultations sont, à ne point douter, des sortes de forums d'experts constitutifs des modalités à travers lesquelles les experts contribuent à la production de l'action publique aujourd'hui. Ils constituent tantôt une résultante de constitution interne de l'expertise, tantôt le résultat de l'extériorisation de celle-ci. Leur fréquence et la qualité de leurs résultats dépendent grandement des financements qui y sont alloués et de la nature du processus de sélection/recrutement des experts. Ainsi, les colloques et conférences scientifiques relatifs aux questions de cybersécurité et de cybercriminalité organisés le plus souvent au sein des universités et des grandes écoles constituent un véritable pilier à travers lequel les experts transmettent leurs connaissances en matière d'action publique de lutte contre le phénomène de cybercriminalité. Parler ainsi ne nous éloigne pas de la perspective en termes de forums développée en politiques publiques par Bruno Jobert (1995) et plus tard par Eve Fouilleux (2003). Le forum est défini comme « une scène plus ou moins institutionnalisée, régie par des règles et des dynamiques spécifiques, au sein desquelles des acteurs ont des débats touchant de près ou de loin à la politique publique que l'on étudie » (*Ibid.,* 278). Il renvoie ainsi à un « lieu » producteur d'idées et de représentations sur une politique (Muller & Boussaguet, 2005) ou un problème public à résoudre. Les colloques et conférences scientifiques se confondent donc aux forums des experts. Ils sont composés d'experts, agissant soit comme spécialistes des questions cybersécuritaires, soit comme des spécialistes de la communication et de l'information, qui vont formuler les conditions techniques optimales du changement de politique, et c'est l'impératif de rigueur scientifique du raisonnement qui oriente les règles de l'argumentation.

Les colloques scientifiques sont en réalité des cadres idéaux pour diffuser des résultats de recherche et débattre entre chercheurs-spécialistes, experts, décideurs sur des questions préoccupantes. Nous avons personnellement pris part du 24 au 25 avril 2018 à un colloque international sur le thème : « Défense nationale : réseaux sociaux et défis sécuritaires » organisé à l'école supérieure internationale de guerre de Simbock-Yaoundé. Des experts se sont réunis pendant ces deux jours pour débattre sur les questions relatives au cyberespace et en trouver des

issues pour la cybersécurité au Cameroun. Voici les thèmes en question qui ont meublé les réflexions des experts lors de ce colloque : « Les technologies de l'information et de la communication face à la protection de la confidentialité de l'information stratégique », « Réseaux sociaux face aux enjeux sécuritaires : témoignages d'acteurs » et « Intégration des réseaux sociaux au profit de la Défense Nationale ».
A l'occasion, il leur a été exhorté de « parvenir à des solutions idoines aux effets pervers des réseaux sociaux qui se constituent de plus en plus en véritables vecteurs de désinformation, de manipulation et de déstabilisation » et d'« envisager des perspectives pour une utilisation et imprégnation de ces (leurs) savoirs ». Dans la même foulée, Galax Yves Landry Etoga, ministre Secrétaire d'État auprès du Ministre de la Défense chargé de la Gendarmerie Nationale formulait, au cours de son allocution, le propos ci-après : « Il s'agira donc pour vous chers experts, de parvenir à des solutions idoines aux effets pervers des réseaux sociaux alors devenus de véritables vecteurs de désinformation, de manipulation et de déstabilisation ». On peut ainsi clairement voir que les colloques et conférences scientifiques ne sont pas simplement des lieux de débats théoriques sans portée pratique, mais des véritables lieux de production des idées pouvant conduire au changement de l'action publique.
Bien plus, la plupart des études faites sur les conseillers des décideurs publics en général s'accordent à dire qu'hier (Lagarde, 2014) comme aujourd'hui, les autorités publiques s'entourent d'un nombre plus ou moins limité de conseillers dans la réalisation de leurs différentes missions. Le conseiller ici est avant tout un expert dans un domaine bien défini (« expert spécialiste »), un « collaborateur de l'ombre » qui n'a pas de vie publique à faire prévaloir (Lagarde, *op.cit.*). Le travail concret des conseillers des autorités publiques, notamment les hauts fonctionnaires, prend la forme d'un accompagnement dans l'optique de leur offrir des meilleures analyses et propositions. L'expert-conseiller est au sein d'une institution celui qui aide à réduire les incertitudes et à dépasser les situations de crise. Il est ainsi un producteur privilégié des bonnes normes professionnelles. Les conseillers sont souvent les plus proches collaborateurs qui proposent des démarches à suivre, des actions à mener, bref ce qu'il faut faire. Ils peuvent être considérés à tort ou à raison comme étant « le cœur », « le ventre », « les yeux », « les oreilles » et souvent « les mains » voire « les pieds » du décideur. Ce sont des personnes aux profils d'études et professionnels riches. L'État s'ouvre à

l'expertise extérieure, de nature privée, produite en partie par les cabinets de conseil, les *think tanks* (centres de réflexions). La vérité étant que, lorsque les autorités militaires et policières font appel à des consultants privés, une logique guide leur choix, celle de la neutralité et de l'impartialité.

Certains experts auprès desquels nous avons mené des enquêtes soulèvent le problème de la prise en compte de leurs idées par les décideurs. Un de nos enquêté en la matière, le docteur Georges Belle, nous confie ceci : « quand bien même nous ne sommes pas consultés par les autorités publiques, nous procédons par l'élaboration des projets que nous soumettons à leur validation. Mais hélas, ces projets sont difficilement bien perçus et validés ». Par ailleurs, le processus de recrutement n'est pas toujours transparent. Très souvent, on note l'absence d'un appel à candidature, et quand bien même il y en a un, la sélection des experts se fait sur la base des affinités communautaires ou par copinage. Ils sont directement recrutés par les institutions spécialisées dans la lutte contre la cybercriminalité évoquée plus haut. Il ne faut donc pas passer un concours pour être recruté comme expert. Dans le cadre d'une enquête sur l'impact de la cybercriminalité que nous avons menée auprès des entreprises à Douala (capitale économique du Cameroun), du 11 juillet 2020 au 26 juillet 2020, sur 40 entreprises enquêtées, 23 nous ont signifié ne pas disposer d'experts en cybersécurité. Ceci témoigne de l'idée que le phénomène de cybecriminalité est peu connu par le public et les entreprises privées. Pour un échantillon de 100 entreprises au Cameroun, 55 disent disposer d'une politique de sécurité du système informatique. « L'expertise profane » tarde encore à se mettre sur pied en matière de cybersécurité. Elle renvoie à l'idée que « des personnes sans formation académique sur un sujet – mais concernées par ce sujet parce qu'elles ont une expérience personnelle – sont capables de développer des connaissances et des analyses spécifiques » (Akrich & Vololona, 2012 : 69) non négligeables pouvant aider à la décision. L'étude menée par l'annuaire statistique des télécommunications et TIC au Cameroun montre que seulement six victimes sur 100 portent plainte (Minpostel, 2017). C'est la preuve qu'un gros travail de sensibilisation reste encore à faire.

2. La collaboration experte comme pilier de rationalisation de l'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route » au Cameroun

Le recours à l'expertise n'a de sens dans l'action publique que s'il contribue à la rendre efficiente (Mintzberg, 1979). De manière générale, il est exprimé par les acteurs en ces termes : « nous voulons atteindre les résultats » ; « nous voulons être précis », « nous ne voulons pas un travail mal fait », « nous voulons faire les choses comme il se doit » etc. Tout semble indiquer que le référentiel principal reste la rationalité en finalité. L'on ne peut ainsi véritablement penser « l'hybridation savoir-pouvoir » (Machikou, 2010 : 165) en faisant abstraction du souci de rationalisation de l'action publique que se font les décideurs publics, et qui constitue l'un des principaux fondements de cette hybridation. Chez Nadine Machikou, le souci de rationalisation constitue, à côté du souci populationnel, une sorte de souci réflexif que se fait l'Etat (Ibid., 126). L'idée est de dire que, pour qu'elle soit rationnelle, l'action publique a besoin d'être fondée sur des connaissances empiriques et les résultats tangibles. Les enquêtes effectuées par les experts en statistiques mettent à la disposition des décideurs politiques les données et les bases de connaissances rationnelles susceptibles de mieux évaluer les effets des politiques entreprises.

2.1. L'expérience chinoise en matière de lutte contre la cybercriminalité

En matière de lutte contre la cybercriminalité, la Chine fait partie des pays du monde qui disposent d'une expertise avérée (Iasiello, 2016 : 45-69). En effet, pour lutter contre la cybercriminalité sur son territoire, la République populaire de Chine a structuré sa politique autour de deux grands dispositifs qui, jusqu'ici, lui ont permis de maîtriser, mieux que les Etats d'Afrique francophone, le phénomène de cybercriminalité. Il s'agit de « la grande muraille » virtuelle et « les trois guerres ».

S'agissant de « La grande muraille » virtuelle, elle a été mise en place en 2003, et s'assigne pour objectif de contrôler les flux d'informations en les obligeant à transiter par des points d'entrée. Grâce à ce dispositif, la Chine traque les hackers y compris les blogueurs malveillants, qui écopent parfois de lourdes peines, comme Dong Rubin, dans le Yunnan, condamné fin juillet à six ans et demi de prison. Quant à la stratégie « les

trois guerres », elle a été adoptée la même année par le Comité central du Parti communiste chinois et la Commission militaire centrale et se veut un outil de guerre d'information non militaire, destiné à être utilisé par l'Armée populaire de libération avant et pendant les hostilités. « Les trois guerres » font référence à la guerre psychologique, la guerre de l'opinion publique et la guerre juridique. La première constitue un instrument de dissuasion, de déstabilisation et de démoralisation des cyber-ennemi(e)s. La deuxième offre à la Chine la possibilité d'influencer l'opinion publique nationale et internationale dans l'optique d'obtenir le soutien des actions militaires de la Chine et dissuader un adversaire de mener des actions contraires aux intérêts de la Chine. Et la dernière justifie la raison des actions menées.

Par ailleurs, la Chine a développé et multiplié des actions de coopération avec plus de 70 pays dans le monde pour lutter contre la cybercriminalité. Ces élans de coopération lui permettent aujourd'hui d'avoir facilement l'information et de mettre main sur les cybercriminels. Dans ce sens, la Chine a entrepris et adopté des projets d'accords sur le cyber sécurité tels que :

-**Le Projet de Code international pour la sécurité de l'information de 2015 :** c'est un projet des Nations Unies initialement signé par quatre Etats, parmi lesquels la Chine. Les trois autres Etats sont : Russie, Tadjikistan, Uzbekistan. Ils ont été rejoints quelques années après par se le Kazakhstan et le Kyrgyzstan. Il s'agit au fond d'un projet initié par l'ensemble des membres fondateurs de l'Organisation de coopération de Shanghai. « Les notions clefs de ce projet sont la sécurité internationale, la stabilité, la paix, les États, les équilibres, la souveraineté, face aux défis posés par l'espace informationnel. La sécurité de l'information comprend les questions liées au cyberespace (l'environnement informationnel est en Chine comme en Russie, un domaine large qui englobe le cyberespace) » (Ventre, 2015 : 95). Par ce projet, la Chine et les autres Etats signataires entende de lutter contre les utilisations criminelles des technologies de l'information et de développer dans leurs territoires respectifs une « culture de la cybersécurité », en conformité avec la résolution de l'Assemblée générale 64/211 intitulée « Création d'une culture globale de cybersécurité ». En sus, ils s'engagent à « interdire toute utilisation des TIC de nature à nuire à la paix et à la sécurité, toute interférence dans les affaires intérieures des États, toute tentative de déstabilisation politique, économique et sociale. Les États ont le droit de

protéger leur espace informationnel et leurs infrastructures d'information critiques de toute menace, interférence, attaque, sabotage » (*Ibid.*).

-**L'accord de cybersécurité Chine-Russie** signé le 30 avril 2015 visant à poser le principe d'une coopération dans le domaine de la sécurité internationale de l'information. La Chine dispose d'un **Livre blanc de la Défense adopté** le 26 mai 2015 dans lequel elle accorde une place majeure au cyberespace qu'il considère comme le nouveau pilier de l'économie, du développement social et désormais nouveau domaine de sécurité nationale. Et d'une loi de cybersécurité nationale de juillet 2015.

2.2. Tirer profit de l'expérience chinoise dans la rationalisation de l'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route en Afrique francophone

L'idée défendue ici n'est nullement de dire que les Etats d'Afrique francophone ne disposent d'aucune expertise en matière de lutte contre la cybercriminalité, mais plutôt de plaider pour une collaboration avec les experts chinois dont l'expertise en la matière semble plus affinée. L'enjeu étant de tirer le maximum d'enseignements et de partager les expériences dans l'optique d'optimiser l'action publique de lutte contre la cybercriminalité le long de « la ceinture et la route ».

Conclusion

Au demeurant, la réflexion a permis de montrer comment produire l'action publique de lutte contre la cybercriminalité le long de l'initiative chinoise « la ceinture et la route » est un exercice aux prises de la complexité et de la technicité. Si hier, les processus d'élaboration et de mise en œuvre des politiques publiques n'engageaient et n'impliquaient que les autorités publiques, aujourd'hui, ils exigent une franche collaboration entre acteurs de diverses sphères. Dans ce concert des acteurs, les experts semblent occuper une place primordiale. Leurs aptitudes à offrir des solutions crédibles et la notoriété scientifique dont ils bénéficient font d'eux des maillons essentiels pour l'ajustement des faiblesses de l'Etat face au risque. La contribution de ces derniers se fait observer dans les processus de formation et d'apprentissage des acteurs engagés dans l'action publique de lutte contre la cybercriminalité. Ils servent de conseils aux décideurs publics et apparaissent tout au moins utiles aux prises de décisions. Pour l'heure, il revient au gouvernement

d'intensifier les campagnes de sensibilisation de la population sur les risques liés à l'utilisation de l'outil Internet afin de leur doter d'une expertise profane en matière de cybersécurité.

Références bibliographiques

Aby Romain (2020), « Cybersécurité et contrôle de la région », in Bertrand Badie (dir.), *Le Moyen-Orient et le monde. L'état du monde 2021,* Paris, La Découverte, 239-245.

Akrich Madeleine et Vololona Rabeharisoa (2012), « L'expertise profane dans les associations de patients, un outil de démocratie sanitaire », *Santé publique*, vol. 24, n° 1, 69-74.

Baumard Philippe, Forgues Bernard (1995), « Internet : un outil transnational au service du commerce », *Décisions Marketing*, n° 5.

Beck Ulrich (2001), *La société du risque : sur la voie d'une autre modernité,* Paris, Aubier.

Beck Urich (2009), *Pouvoir et contre-pouvoir à l'heure de la mondialisation,* Paris*,* Flammarion Champs Essais.

Bindé Jérôme (2005), *Vers les sociétés du savoir, Rapport Mondial de l'UNESCO*, éditions UNESCO.

Cantelli **Fabrizio** (2007), *L'État à tâtons : pragmatique de l'action publique face au sida*, Bruxelles, Peter Lang.

CRESAL (1985), « Situations d'expertise et socialisation des savoirs », Actes de la table ronde des 14 et 15 mars 1985, Saint-Etienne, Editions du CRESAL.

De Maillard Jacques (2010), « Apprentissage », in Laurie Boussaguet (Dir.), *Dictionnaire des politiques publiques : 3e édition actualisée et augmentée,* Paris, Presses de Sciences Po.

Dekker Brigitte, Okano-Heijmans Maaike and Siyi Zhang Eric (2020), "Unpacking China's Digital Silk Road, Clingendael Report, 27 July.

Douzet Frédérick et Géry Aude (2018), « Les aspects juridique et stratégique de la cyberdéfense. Le droit international et la cyberdéfense », in Taillat Stéphane (Dir.), *La Cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, 61-70.

Drucker Peter (1969), *The Age of Discontinuity. Guidelines to our changing society*, New York, Harper and Row.

Filippone (2017), « La Chine impose la géolocalisation des données sur son territoire », https://www.lemondeinformatique.fr/actualites/lire-la-chine-impose-la-geolocalisation-des-donnees-sur-son-territoire-68391.html, publié le 01 Juin 2017
Fouilleux Eve (2003), *La politique agricole commune et ses réformes. Une politique à l'épreuve de la globalisation*, Paris, L'Harmattan.
Haddad Said (2017), « Une grammaire de la cybersécurité française ou la construction d'une stratégie nationale de cyberdéfense (2008-2017) », *Stratégique*, vol. 117, n° 4, 119-135.
https://www.mcafee.com/enterprise/fr-ca/assets/executive-summaries/es-economic-impact-cybercrime.pdf , consulté le 11/05/2022.
Iasiello Emilio (2016), « China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities », Journal of Strategic Security 9, n° 2, 45-69.
Interpol (2020), « Cybercriminalité », [en ligne] https://www.interpol.int/fr/Infractions/Cybercriminalite, consulté le 12/05/ 2022.
Jobert Bruno (1985), « Introduction : Le retour du politique », dans Bruno Jobert (dir.), *Le tournant néo-libéral en Europe,* Paris, L'Harmattan.
Lagarde Romain (2014), *La Présidence des Conseillers. Analyse sociologique de l'entourage de François Hollande Président de la République,* Mémoire de fin d'études de Master 2 en conseil et Expertise de l'action publique, Science po Toulouse, 2014.
Lecalot, « Internet : la Chine entre reprise en main et lutte contre la cybercriminalité », https://www.francetvinfo.fr/sciences/high-tech/internet-la-chine-entre-reprise-en-main-et-lutte-contre-la-cybercriminalite_1710647.html, consulté le 10/05/2022.
Lindblom Charles (1979), « Still Muddling, Not Yet Through », *Public Administration Review*, vol. 6, n° 39, 517-526.
Machikou Nadine (2010), *Les chemins d'un Etat observateur. Contribution des observatoires régionaux de santé,* thèse de Doctorat en Science politique, Université de Picardie Jules Verne.
Massardier Gilles (2003), *Politiques et actions publiques,* Paris, Armand Colin.
Matignon Emmanuel (2012), *La cybercriminalité : un focus dans le monde des télécoms,* Mémoire de master en informatique, Paris.

Mcluhan Herbert Marshall (1977), *Pour comprendre les médias : Les prolongements technologiques de l'homme*, Paris, Seuil.
Minpostel, (2017), Annuaire statistique des télécommunications et TIC au Cameroun, Yaoundé.
Mintzberg Henry (1979), *The Structuring of Organizations,* Prentice Hall, 1979.
Muller Pierre, Boussaguet Laurie (2005), « L'impact du forum politique sur la formulation des politiques publiques », in *Politiques et management public,* vol. 23, n° 3. Le management public à l'épreuve de la politique. Actes du quatorzième Colloque international - Bordeaux, jeudi 17 mars et vendredi 18 mars 2005 organisé en collaboration avec Sciences-Po Bordeaux -Tome 1.
Padioleau Jean-Gustave (2001), « La société de la connaissance et la gestion de sa complexité », Cycle de séminaires Vicente Pérez Plaza, Université technique de Valence.
Tremblay Gaëtan (2016), « Vers des sociétés du savoir : un projet social », *Les Enjeux de l'information et de la communication*, vol. 17, n° 2, 239-249.
Nantulya Paul (2019), "Les activités stratégiques croissantes de la Chine en Afrique reposent sur le hard power chinois", *Éclairage*, Centre d'études stratégiques de l'Afrique.
Sabatier Paul (2000), « Les approches cognitives des politiques publiques : perspectives américaines », *Revue française de science politique,* 50e année, n°2, 209-234.
SHADOW Market 2011 - BSA Global software piracy study Ninth edition, MAY 2012.
Tin Hinane El Kadi, "The Promise and Peril of the Digital Silk Road", Chatham House, 6 June 2019, https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road#, consulté le 10/05/2022.
Tybring-Gjedde Christian (2020), « 2020 - Rapport- initiative la ceinture et la route de la chine : une évaluation stratégique et économique », novembre 2020.
Unicef (2017), La Situation des enfants dans le monde 2017. Les enfants dans un monde numérique, rapport de 2017.
Ventre Daniel (2015), « Cybersécurité : perspectives chinoises », *Revue Défense Nationale*, vol. 785, n° 10, 93-97.

Weber Max (1919), *Le savant et le politique*, Paris, Union Générale d'Éditions, 1919.
Zittoun Philippe (2013), *La fabrique politique des politiques publiques : une approche pragmatique de l'action publique*, Paris, Science Po, Les presses.
Zola Emile (1898), « J'accuse... », *L'Aurore*, le 13 janvier 1898.