Les systèmes nationaux de renseignement en tant que réseaux

Distribution du pouvoir et risque organisationnel au Brésil, en Russie, en Inde, en Chine et en Afrique du Sud

Marco Cepik, PhD*
Gustavo Möller**

La légitimité et l'efficacité des services de renseignement sont plus controversées que jamais. La mondialisation n'a eu pour effet que d'exacerber cette tendance. Premièrement, un plus grand nombre d'acteurs (y compris les entreprises, les groupes non gouvernementaux et les organisations internationales) s'engagent dans des activités de renseignement avec une pléthore de nouvelles ressources technologiques. Deuxièmement, à l'ère numérique, atteindre un juste équilibre entre sécurité et liberté est devenu encore plus difficile. Enfin, pour rappel de la structure anarchique internationale et de ses contraintes politiques, les services de renseignement sont présents partout, à la fois dans les pays démocratiques et dans les régimes autoritaires. Avec la police et les forces armées, ils forment le noyau du pouvoir coercitif de tout état. Souvent, le succès d'un état en matière de renseignement est une atteinte à la sécurité d'un autre état. Leur mission ultime est cependant de fournir des connaissances spécialisées sur les menaces et les vulnérabilités au profit du processus décisionnel relatif à la sécurité nationale. Leur fonctionnement interne, les interactions institution-

*Marco Cepik est professeur agrégé de sécurité internationale et de politique comparée à l'Université fédérale du Rio Grande do Sul (UFRGS), à Porto Alegre, au Brésil. Il a été chercheur invité à l'Université Renmin (RUC, Pékin), à l'Université d'Oxford, à la Naval Post Graduate School (NPS, Monterey, États-Unis), à l'Indiana University of Pennsylvania et à la Latin American Social Sciences School (FLACSO, Équateur).

**Il est directeur du Núcleo de Estudos em Economia Criativa e da Cultura (NECCULT), Faculté d'économie, Université fédérale de Rio Grande do Sul (UFRGS), Porto Alegre, Brésil.

CEPIK, Marco et MÖLLER, Gustavo, « National Intelligence Systems as Networks: Power Distribution and Organizational Risk in Brazil, Russia, India, China, and South Africa », *Brazilian Political Science Review*, 11, n° 1, 2017, e0001. Epub 27 mars 2017, https://dx.doi.org/10.1590/1981-3821201700010001.

nelles et les externalités sont les principaux sujets du champ de recherche interdisciplinaire appelé « Intelligence Studies », l'étude du renseignement. Ce domaine est étroitement lié à des entreprises similaires, telles que les études stratégiques, les études des systèmes de défense et le sous-domaine de la sécurité internationale dans les relations internationales et les sciences politiques.

L'un des sujets d'intérêt permanent pour les études du renseignement est la répartition du pouvoir entre les divers éléments des systèmes de renseignement nationaux contemporains. Comme l'ont souligné Gill et Phythian, l'approche organisationnelle/fonctionnelle des services de renseignement a privilégié l'étude des États-Unis et du Royaume-Uni[1]. L'étude du renseignement a néanmoins également bénéficié de plus de 20 ans de recherche comparative[2]. La plupart des progrès ont été obtenus sur des questions spécifiques telles que la législation, la professionnalisation, le contrôle externe, l'impact du terrorisme et les processus de démocratisation[3]. Deux éléments font principalement obstacle à l'avancement de l'étude comparative du renseignement. Le premier est empirique, car les difficultés d'accès, la désinformation et le secret sont encore plus restrictifs lorsqu'il s'agit d'autres pays. Le deuxième est d'ordre théorique, en raison d'un manque de dialogue entre les explications organisationnelles et interactionnelles (comportementales) de l'évolution des systèmes nationaux de renseignement[4].

Par conséquent, la principale contribution de cet article est de faire progresser la recherche comparative dans le domaine de l'étude du renseignement. L'analyse des réseaux sera utilisée pour évaluer les systèmes nationaux de renseignement au Brésil, en Russie, en Inde, en Chine et en Afrique du Sud. Ces cinq pays sont membres du groupe international BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud), qui regroupe les plus grandes économies en développement du monde. Malgré une grande hétérogénéité des capacités militaires, les perceptions de la menace, les régimes politiques, les positions diplomatiques et les profils économiques, ils forment les états les plus importants du monde contemporain, avec les États-Unis d'Amérique et ses alliés[5]. Bien que les BRICS soient des acteurs notables de la scène mondiale, notre objectif premier n'est pas de comparer la pouvoir de leurs systèmes de renseignement, que soit entre eux ou par rapport aux capacités de renseignement des États-Unis d'Amérique. Notre tâche consiste plutôt à comparer la façon dont le pouvoir est distribué à l'intérieur de chaque système national. Nous avons ainsi essayé de répondre à trois questions : 1. Comment les systèmes nationaux de renseignement sont-ils organisés dans les cinq pays ? 2. Comment le pouvoir est-il réparti entre les différents organismes de chaque système national de renseignement ? 3. Quelles sont les implications d'une distribution donnée du pouvoir sur le risque organisationnel global du système ?

Nous définissons les systèmes de renseignement comme des réseaux composés de nœuds (organisations) et de liens (relations), ce qui nous permet de considérer les asymétries d'autorité et de contrôle de l'information comme des indicateurs de la distribution du pouvoir dans un réseau donné. Trois types d'organisations seront analysés : la supervision (gouvernement), la coordination (organes collégiaux) et la mise en œuvre (agences). Un quatrième type d'organisation, à savoir les organismes de contrôle externe (contrôle), n'a pas été inclus, par souci de brièveté. Les données empiriques de chaque pays proviennent de documents publics, de la législation et des informations issues des médias. Nous sommes conscients des limites imposées par l'utilisation de ces sources. Néanmoins, les graphiques et les matrices de contiguïté utilisés en analyse de réseau sont meilleurs que les organigrammes traditionnels pour décrire les systèmes de renseignement, parce qu'ils permettent la représentation des relations mutuelles entre les nœuds du réseau[6]. De plus, une fois que la compréhension de la distribution du pouvoir à l'intérieur du réseau acquise, on peut expliquer des éléments tels que le risque organisationnel, qui est une gamme d'effets allant de légères difficultés à réaliser la coopération à de graves difficultés à s'adapter à de nouveaux défis stratégiques, entraînant une fragmentation potentielle du réseau[7].

Dans la section suivante, nous expliquons les méthodes utilisées pour répondre aux questions de recherche, y compris les définitions, les choix techniques et les procédures de collecte des données, les calculs, la vérification des résultats et l'analyse des écarts. Nous présentons ensuite les résultats obtenus pour chacun des cinq pays (Brésil, Russie, Inde, Chine et Afrique du Sud). Dans la dernière section, nous comparons les résultats obtenus pour chaque pays afin de répondre aux questions de recherche et indiquer les limites et les défis pour la prochaine série d'études comparatives relatives aux services de renseignement.

Méthodologies

Les réseaux sont formés par des nœuds (aussi appelés sommets) et des liens (aussi appelés arêtes). Les nœuds peuvent être des personnes, des villes, des connaissances, des ressources ou tout autre objet matériel ou immatériel que l'on choisit d'analyser. Dans le cas des systèmes nationaux de renseignement, tous les nœuds appartiennent à une seule classe : les organisations. Comme les organisations sont des acteurs collectifs, tout au long de l'article, les termes nœud, acteur et organisation seront utilisés de façon interchangeable. Pour qu'un réseau existe, les nœuds doivent être reliés au moyen d'un flux ou d'une liaison. Les liens entre les nœuds peuvent être dirigés (indiqués par une flèche) ou non dirigés (réci-

proques). Pour l'analyse des systèmes nationaux de renseignement, nous avons examiné à la fois les liens dirigés (autorité) et les liens non dirigés (flux d'information).

Par autorité, nous entendons la subordination hiérarchique exercée par une organisation par rapport à une autre. Dans le cadre d'un état contemporain, même les relations professionnelles (des experts sont invités à fournir des informations au lieu de recevoir des instructions unilatérales) dans le domaine du renseignement se déroulent dans un cadre bureaucratique et au moins partiellement formel. De leur côté, les flux d'information entre les organisations ont été évalués en fonction des obligations officielles en matière d'établissement de rapports, des doubles appartenances ou d'autres sources spécifiques à chaque pays. Ensemble, les flux d'autorité et d'information équivalent à une définition relationnelle du pouvoir[8]. En d'autres termes, le pouvoir découle de la position d'un acteur dans le réseau. Cette position est déterminée par le nombre et l'intensité des relations subordonnées dont l'acteur fait l'expérience. De plus, la position de l'acteur est également déterminée par le nombre et l'intensité des flux d'informations qu'il intercède.

En analysant les données obtenues à partir de documents publics et de informations médiatiques, l'autorité exercée par chaque organisation a été évaluée par les auteurs sur une échelle de quatre intervalles (0, 03, 06 et 09). L'intensité 09 indique les relations prévues par la loi et jugées efficaces, c'est-à-dire le pouvoir de demander à d'autres de recueillir et d'analyser des informations ou d'agir sur la base de ces informations, ce qui est à la fois autorisé par la loi et réalisé sans insubordination significative. Les relations d'autorité d'intensité 06 sont celles prévues par la loi, mais dans lesquelles il y a des limitations sur le degré de subordination observé, soit dans des sujets spécifiques, soit sur des périodes de temps spécifiques. Un niveau d'autorité 03 est un niveau d'autorité prévu par la loi, mais caractérisé par une insubordination ou une marge de manœuvre importante. Elle peut aussi représenter une situation où l'organisation est légalement soumise à un acteur particulier, mais officieusement, c'est un autre acteur qui la subordonne. Elle peut aussi exprimer un renversement de la direction du commandement. Nous appliquons « 0 » lorsqu'il n'existe aucune relation entre les organisations ou lorsqu'elle n'est pas pertinente pour le fonctionnement du système national de renseignement.

La même échelle a été utilisée pour évaluer l'intensité du flux d'information. Les relations dont l'intensité a été classée en 09 sont celles où le flux d'information est couvert par la loi et où il est prouvé qu'il est efficace entre deux nœuds du réseau. L'intensité 06 indique quant à elle un flux d'information couvert par la loi, mais inefficace pour diverses raisons (faibles taux de partage, concurrence entre agences, règles administratives de compartimentation, etc.) Une intensité 03 a été attribuée aux flux d'information qui ne sont pas couvert par la loi, mais dont

l'existence entre deux acteurs est prouvée. Nous appliquons « 0 » lorsqu'il n'y a pas de flux d'informations pertinents entre deux nœuds du réseau.

Les données primaires sur les services de renseignement sont de nature qualitative et proviennent de sources publiques, comme les documents officiels, la législation, les livres, les articles et les informations médiatiques[9]. Dans le cas des pays BRICS, décider des organisations constituant un système national de renseignement présente quelques difficultés[10]. Lorsqu'elles sont disponibles, les définitions juridiques déterminent les organisations qui font partie du système national de renseignement. Lorsqu'il n'y avait pas de base légale pour décider des composantes du système, nous avons utilisé la proximité thématique d'une organisation par rapport aux questions de sécurité nationale en vue de son inclusion ou non. Ainsi, de nombreux organismes dont les activités sont axées sur le renseignement criminel, surtout au niveau local, n'ont pas été inclus dans le réseau. De même, les organisations privées et non gouvernementales ont été exclues, même si nous reconnaissons l'importance croissante et la nécessité d'effectuer des recherches supplémentaires à leur sujet[11]. Les task forces, les centres de fusion et les groupes de travail ont également été exclus du réseau. Nous sommes conscients de leur importance croissante dans de nombreux pays. Cependant, leur nature temporaire et parfois « ad hoc » rend la compilation d'informations en suffisance difficile à ce stade. Dans le cas des forces de police et militaires dispersées sur l'ensemble du territoire et dotées de systèmes divisionnaires très complexes, nous avons décidé de les regrouper par fonctionnalité et subordination au niveau national (voir Résultats par pays). Tous les nœuds de réseau appartiennent à la même classe (organisations), mais ont été classés en trois grands types : supervision (gouvernement), coordination (organes collégiaux) et mise en œuvre (agences). Comme nous l'avons déjà mentionné, nous continuons de recueillir des données sur un quatrième type d'organisation très pertinent dans les systèmes de renseignement, à savoir les organismes de contrôle externe (commissions parlementaires, tribunaux spéciaux, etc.).

Une fois que les organisations qui forment le système national de renseignement d'un pays établies, nous avons également pondéré l'intensité d'une relation donnée entre deux organisations données à l'intérieur de ce système. Par exemple, la relation d'autorité entre une organisation collégiale (coordination) et les autres nœuds du réseau n'a été classée comme intensité 09 que lorsqu'un membre de l'organisation membre de l'organe collégial avait le pouvoir de dissoudre ce dernier, combinant à la fois les rôles de coordination et de commandement. Dans d'autres cas, ce type de nœud a toujours vu ses relations d'autorité classées au grade 06. Les relations d'autorité du chef de l'état avec d'autres nœuds relevant du type des organisations gouvernementales de supervision et de direction ont été

classées au grade 09, à l'exception de certains cas, sur la base de preuves que nous détaillons dans le présent article. Enfin, bien que les task forces, les centres de fusion et les groupes de travail n'aient pas été inclus en tant que nœuds du réseau, leur existence a néanmoins été prise en considération, compte tenu de l'intensité attribuée aux relations de flux d'information entre les nœuds participants du groupe de travail.

Une fois que toutes les composantes d'un système national de renseignement (les nœuds du réseau) ont été identifiées et classées, leurs relations mutuelles ont été enregistrées dans deux matrices, l'une pour les relations d'autorité et l'autre pour les flux d'information. Les matrices d'adjacence sont une façon de représenter un réseau. Dans ce cas, les mêmes acteurs (ou nœuds de réseau) sont disposés selon deux axes, avec des lignes et des colonnes formant un carré. Dans les cellules de la matrice, chaque relation entre deux acteurs est enregistrée selon leur échelle d'intensité. Naturellement, les cellules diagonales qui coupent le tableau en deux (reliant chaque acteur à lui-même) sont remplies par un « 0 ». Les matrices servent de base à l'enregistrement des données, à la génération de graphiques et à l'exécution des calculs[12]. Tous les travaux ont été réalisés à l'aide du logiciel ORA (Organizational Analyzer), développé par le Center for Computational Analysis of Social and Organizational Systems (CASOS) de l'Université Carnegie Mellon[13].

Afin de répondre à la question de recherche sur la répartition du pouvoir dans chaque système de renseignement national, deux indices de centralité différents ont été calculés pour chaque nœud. Selon Brandes et Erlebach, différents indices de centralité permettent d'observer différents aspects des relations de pouvoir dans un réseau[14].

L'indice de centralité des degrés, par exemple, est défini comme le nombre de liens entre un nœud et les autres, c'est-à-dire la façon dont un nœud est connecté. Dans les graphiques dirigés, tels que ceux générés par la matrice d'autorité, nous avons deux mesures de centralité, une relation de calcul dans laquelle l'acteur est subordonné (en degré), et d'autres relations dans lesquelles l'acteur est subordonné à un autre (hors degré). Par conséquent, la centralité des degrés est un indice composite, qui peut être décomposé en mesures en degrés, hors degrés et en mesures de degrés totaux. Plus la distribution relative des connexions d'un nœud (organisation) est élevée, moins il devient dépendant d'un autre nœud spécifique[15].

L'indice de centralité d'intermédiarité entre les nœuds est obtenu en calculant le nombre de fois qu'un nœud donné intercède la relation entre d'autres nœuds sur un chemin géodésique (le chemin le plus court entre deux nœuds). Cet indice nous permet d'évaluer quels nœuds (acteurs) se trouvent en position de partie prenante, c'est-à-dire quels nœuds ont le pouvoir de retenir l'information au

sein du réseau et le potentiel de rompre ou d'empêcher les relations, isolant ainsi d'autres acteurs[16].

Tout d'abord, chaque indice de centralité (degré et intermédiarité) a été calculé séparément pour chaque nœud (organisation) du réseau. Ensuite, les résultats ont été normalisés sur une échelle comprise entre 0 et 100, ce qui a permis d'égaliser la taille des différents systèmes nationaux de renseignement, ce qu'on appelle techniquement le diamètre du réseau. La normalisation a été obtenue en additionnant les indices obtenus pour chaque acteur, puis en divisant l'indice individuel de chaque acteur par la valeur de la somme de tous les acteurs. Enfin, les indices normalisés ont été comparés pour établir la position relative (pouvoir) de chaque acteur du réseau. La méthode combine ainsi des étapes qualitatives et quantitatives. Les étapes qualitatives sont cruciales et déterminent le processus, bien que le choix des indices et des calculs appropriés constitue également une partie importante de la méthodologie.

Pour répondre à la question de recherche portant sur le risque organisationnel d'un système national de renseignement en raison d'une répartition donnée du pouvoir, deux indices supplémentaires ont été utilisés, conformément à McCulloh, Armstrong et Johnson[17]. Gardons à l'esprit que par risque organisationnel, nous entendons la probabilité que la distribution interne du pouvoir produise dans le système une gamme d'effets allant de légères difficultés à réaliser la coopération inter-agences à de graves difficultés à s'adapter à de nouveaux défis stratégiques, entraînant une fragmentation potentielle du réseau. Malheureusement, la méthodologie ne permet pas d'établir quels effets en découleront ou la façon dont le gouvernement national respectif y réagira[18]. De plus, il est important de noter que la littérature sur l'analyse de réseau utilise des noms similaires pour les indices supplémentaires. Bien que cela puisse être un peu déroutant, souvenons-nous simplement que si les indices précédents ont été calculés pour chaque nœud du réseau, ces deux nouveaux indices sont appliqués à l'ensemble du réseau (analyse au niveau du graphique).

L'indice de centralisation des degrés indique l'existence de nœuds (organisations) très centraux dans le réseau. De tels nœuds, s'ils étaient supprimés, entraîneraient la dispersion des autres. Le calcul de la centralisation des degrés a été appliqué aux relations d'autorité. Cet indice est mesuré sur une échelle de 0 à 01. Plus un réseau est proche de zéro (0,00), plus il est résilient ou moins sujet à la fragmentation. Il convient aussi de souligner qu'une résilience moindre peut aussi signifier une moindre capacité à s'adapter aux nouveaux défis stratégiques[19]. La signification exacte d'un indice particulier nécessite par conséquent une analyse qualitative supplémentaire.

L'indice de centralisation d'intermédiarité indique la façon dont l'information est répartie uniformément sur le réseau. Il est également mesuré sur une échelle de 0 à 01. Le calcul de la centralisation d'intermédiarité a été appliqué aux relations d'autorité. Plus on se rapproche de zéro (0,00), meilleure est la distribution de l'information. De toute évidence, pour des raisons de sécurité, dans le cas des systèmes nationaux de renseignement, une diffusion totalement égale de l'information sur l'ensemble du réseau n'est pas nécessairement souhaitable ou possible. D'autre part, plus on se rapproche de 1 (1,00) en termes de centralisation d'intermédiarité, plus le risque qu'une organisation à nœud unique puisse conserver toute l'information, agissant en tant que gardien du réseau, sera élevé.

Nous avons calculé chaque indice de centralisation (degré et intermédiarité) séparément. Comme les deux indices sont déjà exprimés sur une échelle comprise entre 0 et 01, il n'était pas nécessaire d'effectuer la procédure de normalisation. Vous trouverez, dans les sections suivantes, les résultats préliminaires relatifs aux systèmes nationaux de renseignement du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud[20].

Brésil

Créé en 1999 par la loi fédérale 9 883, l'actuel système brésilien de renseignement (SISBIN) a été caractérisé par une continuité organisationnelle et des crises institutionnelles récurrentes[21], notamment en raison du fait que la législation brésilienne préfère utiliser des définitions du renseignement et des menaces relativement larges[22]. En dépit de l'existence relativement fréquente dans de nombreux pays (le Royaume-Uni, par exemple) d'une définition—plus ou moins précise—du renseignement, deux particularités institutionnelles se dégagent du cas du Brésil : le haut degré d'inclusion du système de renseignement brésilien et la difficulté de définir des missions axées sur la sécurité nationale[23]. Au total, le système national brésilien de renseignement comprenait 22 organismes de supervision et de direction (gouvernement), 5 organismes collégiaux (coordination) et 23 organismes de renseignement (agences)[24].

Au Brésil, le président a le plus haut niveau d'autorité formelle sur le système (une centralité des degrés de 22,37). Le ministère de la Justice est l'acteur ayant le deuxième niveau le plus élevé (7,34). Cela s'explique en partie par le fait que le président subordonne directement toutes les autres organisations gouvernementales de supervision et de direction (gouvernement). Comme le système brésilien est très inclusif, bon nombre de ces organisations n'ont pas d'activités de renseignement comme mission principale. L'Agence brésilienne du renseignement (ABIN) est un nœud critique. Désigné par la loi comme centre du système de renseignement, son leadership est entravé par des questions liées au budget, aux

priorités stratégiques et à l'orientation de sa mission principale, ainsi qu'au personnel et à l'autorité administrative. Depuis 2002, l'ABIN est placé sous l'autorité du Cabinet de sécurité institutionnelle (GSI) de la présidence. Tant pour sa position intermédiaire dans la chaîne de commandement entre la présidence et l'ABIN que pour sa participation à de nombreuses organisations collégiales de coordination (coordination), le GSI accumule un grand pouvoir au sein du SISBIN[25]. Alors que la centralité des degrés de l'ABIN est de 1,74, le même indice atteint 3,84 dans le cas de l'ICF. Pour accroître la coordination sectorielle, préserver l'autonomie et élaborer des doctrines spécifiques pour le renseignement militaire et de sécurité publique, de nouvelles organisations collégiales ont été créées au début des années 2000 pour la coordination, dont le Système de renseignement de défense (SINDE) et le Sous-système de renseignement de sécurité publique (SISP). Respectivement, le ministère de la Défense (5,24) et le ministère de la Justice (7,34) ont un haut degré de centralité en raison de leur rôle dans ces sous-systèmes[26]. Le ministère des Finances a également un indice de centralité élevé (4,89), ce qui indique une tendance à l'institutionnalisation d'un sous-système de renseignement financier au Brésil.

En ce qui concerne le contrôle des flux d'information, l'ABIN se distingue par une centralité d'intermédiarité de 32,3. Bien qu'elle ait un faible indice de centralité des degrés, cette organisation a des liens avec la plupart des acteurs qui entretiennent des liens avec d'autres acteurs, ayant ainsi le chemin géodésique le plus court et le plus évident comme le montre le flux d'information. Par conséquent, l'ABIN a du pouvoir dans le système non pas en raison du nombre d'organisations qu'il subordonne, mais en raison de son rôle dans la circulation de l'information. Compte tenu de la densité du réseau, l'ABIN ne peut se positionner en tant que gardien du réseau, c'est-à-dire en tant qu'acteur susceptible d'entraver la circulation de l'information[27].

En résumé, le pouvoir est fortement concentré dans le système de renseignement brésilien, même si le système lui-même n'est pas très puissant en raison de son caractère excessivement inclusif et de l'absence de contrôle externe efficace. Seuls quelques acteurs détiennent la majorité des ressources de pouvoir (autorité et information), parmi lesquels le président, l'ABIN et les ministres de la Sécurité institutionnelle, des Finances et, dans une moindre mesure, de la Justice et de la Défense.

Russie

Depuis la fin de l'URSS, la structure du système de renseignement national russe a oscillé en fonction de l'évolution des capacités de l'état, des menaces pour les intérêts nationaux et de la disponibilité des ressources. Depuis l'élection prési-

dentielle de Vladimir Poutine en 2000, l'héritage de Boris Eltsine a été renversé. Au lieu de fragmentation et d'affaiblissement des services de renseignement, on a assisté à une période d'augmentation du pouvoir et des ressources, en particulier après la deuxième guerre en Tchétchénie (1999-2009). On observe une réduction du nombre d'organismes de renseignement, le remplacement de plusieurs directeurs et l'expansion des capacités opérationnelles, des missions et de la base technologique[28]. Plus récemment, malgré la crise en Ukraine et la tension accrue avec l'Union européenne et les États-Unis, l'expansion du système de renseignement russe a été freinée par la crise économique. La base juridique du fonctionnement du système de renseignement russe est un ensemble de lois adoptées en février 2006 (lutte contre le terrorisme, activités de recherche opérationnelle, sécurité), qui s'applique à toutes les organisations de renseignement du pays. Elles complètent les lois spécifiques intitulées sur le Service fédéral de sécurité (mai 1995) et le Renseignement extérieur (décembre 1995). D'autres lois, décrets et directives présidentielles existent par ailleurs. Selon Soldatov, les réformes majeures dans les services secrets russes ne découlent pas du 11 septembre, mais de l'attaque des insurgés en Ingouchie en juin 2004[29]. Au total, la matrice d'adjacence (et le graphique qui en résulte) du système national de renseignement de la Russie comprenait 6 organismes gouvernementaux de supervision (gouvernement), aucun organe collégial (coordination) et 7 organismes de renseignement (agences).

Dans le cas des relations d'autorité au sein du système de renseignement russe, le président a le degré le plus élevé de centralité (36,84). Après les réformes de 2006, le président a concentré encore plus d'autorité, subordonnant directement la plupart des organisations du réseau russe. Bien que le Service fédéral de sécurité (FSB) soit considéré comme un acteur central, son indice de centralité des degrés de 3,95 est inférieur à celui du Service fédéral de contrôle technique et des exportations (FCTEK) (5,26) et égal à des organisations telles que le Service du renseignement étranger (SVR), la Direction du renseignement militaire (GRU), le Service fédéral de protection (FSO), la Direction de la topographie militaire (VTU), ou même le ministère de l'intérieur (MVD) et le Premier ministre. Outre le président, le chef d'état-major des forces armées (13,16) et le ministère de la Défense (9,21) occupent une place centrale dans le système russe.

En ce qui concerne la circulation de l'information, la GRU a la plus haute centralité d'intermédiarité (30,91) dans le système russe, plus élevée même que le FSB (22,55). Une partie de l'explication réside dans le fait que de nombreux flux d'information qui passent par le FSB sont informels, avec une intensité 03 seulement. En revanche, les flux d'information à travers la GRU sont plus formels et, par conséquent, plus intenses. En plus de ces organes, le FCTEK a également un indice de Centralité d'intermédiarité relativement élevé (16,48). Cela peut s'expli-

quer le rôle qu'elle joue dans la sécurité de l'information et le contre-espionnage des signaux. Ce type de mission oblige le FCTEK à maintenir la communication (flux de données) avec les différents acteurs de type 01 (gouvernement) et certaines organisations importantes de type 03 (agences). Enfin, l'indice de centralité du président (14,67) s'explique par le fait qu'il subordonne directement toutes les autorités politiques et toutes les agences, à l'exception de la GRU et de la VTU, ce qui fait que le bureau du président est un intermédiaire naturel dans de nombreuses relations.

La distribution du pouvoir dans le système de renseignement national russe est fortement concentrée sur le président. Il convient de noter que les organisations de type 02 (coordination) n'ont pas été incluses dans le système russe, étant donné les difficultés à obtenir des informations sur le rôle possible du Conseil national de sécurité par rapport aux organisations de renseignement (agences)[30]. Notons encore que la plupart des agences du système sont directement subordonnées au président. Les deux seuls organismes qui ne sont pas directement subordonnés sont la GRU et la VTU, responsables du renseignement par imagerie (IMINT). Les deux organisations sont directement subordonnées au chef d'état-major (CGS) qui, bien que subordonné au ministère de la Défense, est nommé par le président.

Enfin, un mot sur la centralité du FSB, l'organisation responsable du contre-espionnage, du contre-terrorisme et de la protection de la constitution. Vladimir Poutine a été directeur du FSB de 1998 à 1999. Pendant la majeure partie de son mandat de président, le FSB s'est renforcé et a acquis plus de pouvoir. Les agents du FSB ont assumé des postes clés au sein du MDV et ont également développé des activités de renseignement dans les domaines relevant des attributions de la SVR et de la GRU, en prenant même la responsabilité du contrôle des frontières[31]. Toutefois, dans le contexte de la crise ukrainienne, le président russe peut promouvoir des réformes afin de réduire le rôle central du FSB dans le système de renseignement russe.

Inde

Le système de renseignement national indien est fortement guidé par les défis de sécurité régionale, mais aussi par l'objectif de Delhi de devenir une grande puissance[32]. Le large éventail d'organisations du système découle de trois facteurs principaux, à savoir la combinaison des menaces à la sécurité intérieure (insurrection et violence communautaire), les conflits frontaliers (en particulier avec le Pakistan) et les ambitions régionales et mondiales (positionnement vis-à-vis de la Chine et des États-Unis). Jusqu'à présent, l'Inde ne dispose ni d'une législation spécifique réglementant les opérations et les activités de ses services de renseigne-

ment diversifiés, ni de mécanismes de contrôle externe importants ou de surveillance par le Congrès. Par conséquent, la définition de la taille du système de renseignement et de ses relations internes constitue un défi en soi[33]. Heureusement, puisque les agences de renseignement en Inde sont des acteurs actifs du processus politique interne du pays, leur rôle fait l'objet d'un débat considérable dans les médias[34]. La dernière réforme du système date de 2002, lorsque le rapport du Comité Kargil a recommandé des changements qui ont été partiellement mis en œuvre à l'horizon 2008[35]. Au total, la matrice d'adjacence (et le graphique qui en résulte) du système national de renseignement de l'Inde comprenait 7 organismes gouvernementaux de supervision (gouvernement), 2 organes collégial (coordination) et 20 organismes de renseignement (agences).

Du point de vue des relations d'autorité, il est important de souligner dans le cas indien l'indice de centralité des degrés du Premier ministre (14,29). Cela peut s'expliquer par les relations de travail étroites du Premier ministre avec d'autres organismes de supervision (gouvernement), tels que le ministère de la Défense (12,50) et le ministère des Finances (12,50). L'Inde dispose d'agences de renseignement subordonnées au ministère des Finances, dont la plus importante est l'Office central de renseignement économique (CEIB)[36]. De même, la centralité des degrés du ministère de la Défense est élevée parce que ce dernier subordonne un certain nombre d'agences qui forment un groupe de renseignement militaire. Le ministère de l'Intérieur (Affaires intérieures) a un indice de centralité des degrés de 5,3, tandis que l'indice du Bureau du renseignement est de 4,76. Nous pourrions nous attendre à ce que l'indice du ministère de l'Intérieur soit sensiblement plus élevé que celui du Bureau du renseignement (IB). Cependant, les résultats réels reflètent la double subordination de l'agence au ministre et au Premier ministre, ce qui élève le degré de centralité de l'IB. L'organe collégial indien le plus important (coordination) devrait être le Comité conjoint de renseignement (JIC). Ce dernier est subordonné au Conseil national de sécurité (4,79) et se compose des directeurs de la Section de recherche et d'analyse (RAW) (3,57), du Bureau du renseignement (IB) (4,76), de l'Agence de renseignement de défense (DIA) (1,79), des trois officiers du renseignement militaire, d'un haut représentant du ministère de la Défense et d'un haut représentant du ministère des Affaires étrangères. Cependant, le JIC a un indice de centralité des degrés relativement faible (1,79), Ce qui peut indiquer que ce dernier n'a pas été en mesure d'assurer une coordination efficace, principalement en raison de la réduction de son personnel et de la faible fréquence des réunions[37].

En raison de la taille du système, la centralité d'intermédiarité du réseau indien se concentre au sein des clusters du système. Les indices les plus élevés proviennent du Centre national d'anti-terrorisme (NCTC), qui atteint 20,50. Il

communique étroitement avec les autres agences sur la question spécifique de la lutte contre le terrorisme. On notera également le JIC, avec un indice de 13,71 et, encore une fois, le cluster de renseignement économique et fiscal, avec des centralités d'intermédiarité de 13,71 (CEIB) et de 9,78 (ministère des Finances), tous deux plus élevés que celui du Premier ministre (8,21). Les centralités d'intermédiarité entre les agences de renseignement (organisations de type 03), sont relativement faibles, mais significatives dans le cas des agences de cluster de défense, la RAW (4,68), la DIA (3,87), le JCB (3,87), et l'Organisation nationale de recherche technique (NTRO) (3,87).

Dans l'ensemble, la répartition de l'autorité et la circulation de l'information dans le système indien indiquent que le pouvoir est fermement détenu par les organismes de supervision du gouvernement (gouvernement), avec un rôle limité joué par les organismes de coordination (type 02). Il existe également des groupes de pouvoir bien définis dans les domaines de la défense, de la lutte contre le terrorisme et des finances. Le cluster du renseignement financier exige des recherches supplémentaires, mais son pouvoir semble être important. Les quatre principaux organismes de renseignement du système indien sont l'IB, la RAW, la NTRO et la DIA. Le Bureau du renseignement (IB), subordonné au Centre national d'antiterrorisme (NCTC), est l'organisme chargé de faire face aux menaces à la sécurité intérieure et le principal résultat de la réforme post-Mumbai. La RAW est l'agence de renseignement étranger et son importance réelle au sein du pouvoir étatique en Inde semble contraster avec ses indices relativement bas en termes d'autorité et de contrôle de l'information. L'IB et la RAW sont subordonnés au Premier ministre. Dans la mesure où ils jouiraient—dit-on souvent—d'une autonomie considérable, ces divergences entre informations informelles et arrangements institutionnels formels doivent être analysées par le biais de recherches supplémentaires. Enfin, les deux agences de renseignement militaire les plus importantes sont la NTRO, dédiée aux moyens techniques de collecte, et la DIA, qui imite le modèle américain de consolidation des contributions des trois forces armées.

Chine

Le système national de renseignement de la Chine défie toute classification, principalement en raison de sa complexité et de son incommensurabilité par rapport aux États-Unis d'Amérique, au Royaume-Uni ou même aux autres pays du BRICS. Cependant, une première étape doit être d'éviter d'inclure tous les organes de l'état et du parti communiste en tant qu'« organisations de renseignement potentielles[38] ». Il ne s'agit pas de négliger le rôle central joué par le Parti communiste chinois (PCC) dans le système politique ainsi que dans la société chinoise, ni d'ignorer le statut de grande puissance du pays (semblable aux États-Unis et à

la Russie). La Chine dispose probablement d'un très grand système de renseignement, avec des organisations spécialisées axées sur les questions de sécurité interne, régionale et mondiale. La continuité étatique historique en Chine, ses caractéristiques culturelles ou même l'influence soviétique au XXe siècle ne doivent pas occulter le fait que les missions militaires modernes, la police, la politique étrangère, le développement et d'autres appuis du système de renseignement en Chine sont identiques à ceux que l'on retrouve dans d'autres pays. Ce système moderne de renseignement national a vu le jour en même temps que la modernisation militaire, initiée dans les années 1980[39]. Au total, notre décompte du système national de renseignement de la Chine comprenait 10 organismes gouvernementaux de supervision (gouvernement), aucun organe collégial (coordination) et 24 organismes de renseignement (agences)[40].

Sur le plan constitutionnel, le rôle du Président de la République, du Président de la Commission militaire centrale (CMC) et du Secrétaire général du Parti communiste chinois (CPCSG) ne doit pas nécessairement être détenu par la même personne. Le fait que ces rôles soient désormais assumés par une seule personne représente un arrangement politique et institutionnel « de facto ». Compte tenu des relations d'autorité avec les différents nœuds du réseau, l'indice de centralité des degrés du président (7,41) est plus élevé que celui du CPCGS (5,09). De plus, les deux ont des indices plus bas que la CMC (11,11), et un indice encore plus bas que celui du ministère de la Sécurité de l'État (18,52). Cette situation découle en partie de la décision des auteurs de considérer les principaux ministères du MSS comme des entités distinctes. D'autres ministères importants sont le ministère de l'Industrie et des technologies de l'information (MIIT) (4.63), le ministère des Affaires étrangères (MOFA) (3,24) et le ministère de la Sécurité publique (MPS) (2,78). Comme dans le cas de la Russie, les organisations de type 02 (coordination) n'ont pas été identifiées. Compte tenu de la forte spécialisation fonctionnelle du réseau (division du travail entre les nœuds) et du grand nombre d'agences, les indices de centralité des degrés restent faibles pour toutes les organisations de type 03 (agences), allant de 1,39 à 2,78.

Bien qu'il soit très difficile d'estimer le flux d'information dans le renseignement chinois, la configuration du système organisationnel indique que certaines organisations établissent très probablement différents degrés de communication avec d'autres. Les valeurs particulièrement élevées de l'indice de centralité d'intermédiarité du ministère de la Sécurité de l'État (36,62) et du Secrétaire général du CPC (27,19) en sont des exemples. Tous les autres nœuds du réseau présentent une variation de leurs indices de centralité d'intermédiarité allant de 0 à 5,89, dont la présidence (2,19) et la Commission militaire centrale (2,86).

Compte tenu de la performance des deux indices et de ce que l'on trouve dans d'autres pays, trois acteurs (nœuds) concentrent beaucoup de pouvoir dans le système de renseignement national de la Chine, à savoir le MSS et, dans une moindre mesure, le président et la CMC. Dans le cas de la CMC, la chaîne de commandement du groupe de renseignement militaire comprend les départements généraux (Département politique général[GPD] ; Département d'état-major général[GSD] ; 2ème Département[GSD2] ; et 3ème Département[GSD3]), ainsi que les capacités de renseignement des quatre forces de l'Armée populaire de libération (PLA), à savoir les forces terrestres, la marine, la force aérienne et la seconde force d'artillerie. ON remarquera aussi que les capacités de renseignement de la Police armée populaire (PAP), principale force de l'ordre du pays, sont subordonnées à la fois au MPS et à la CMC. De son côté, le MSS et ses différents départements (bureaux) correspondent à un important pôle de renseignement civil. Enfin, contrairement à d'autres pays où un cluster de renseignement financier ou fiscal semble prendre une forme institutionnelle, la Chine se distingue par l'importance croissante du GSCPC et du MIIT.

Afrique du Sud

Après la défaite du régime de l'apartheid, le système national de renseignement de l'Afrique du Sud a fait l'objet de deux réorganisations majeures. En 1996, la nouvelle constitution a établi deux principes de base pour le fonctionnement démocratique du renseignement sud-africain : la coordination entre les agences et le contrôle civil de leurs activités. Au milieu des années 1990, la loi sur le renseignement et le Livre blanc sur le renseignement ont précisé la division des missions de renseignement en agences distinctes (internes et externes), en mettant l'accent sur les mécanismes de contrôle externe, la coordination, la supervision et l'utilisation des moyens techniques de collecte. En 2005, des plaintes relatives à des opérations illégales d'interception de communications de membres de l'ANC (le parti au pouvoir) ont porté atteinte à la légitimité des services de renseignement et de leurs organes de contrôle[41]. En 2009, le nouveau président Jacob Zuma a annoncé des changements dans le système de renseignement qui, à l'horizon 2013, seront régis par l'amendement modifiant la Loi sur le renseignement général. Les nouvelles structures ont été conçues pour produire une consolidation administrative, réduire le nombre d'agences et se recentrer sur des missions strictement liées à la sécurité nationale[42]. Au total, la matrice d'adjacence (et le graphique qui en résulte) du système national de renseignement de l'Afrique du Sud comprenait 5 organismes gouvernementaux de supervision (gouvernement), 2 organes collégiaux (coordination) et 11 organismes de renseignement (agences).

En termes d'autorité, l'indice de centralité du Président sud-africain (18) est inférieur à celui de l'Agence de sécurité de l'état (SSA) (20). Bien que le président subordonne tous les ministères et n'est subordonné à aucun autre nœud du réseau—ce qui rend son degré supérieur à celui de la SSA—le degré total est inférieur en raison de la prise en compte par l'indice composite de toutes les relations subordonnées dans lesquelles un acteur est impliqué. Comme la SSA relève du président et du ministère de la Sécurité de l'État, mais subordonne les six branches qui le composent depuis la réforme de 2009, sa centralité des degrés est plus élevée. Toutes les autres organisations du système de renseignement de l'Afrique du Sud ont des indices de centralité des degrés allant de 02 à 07.

Le président a le plus grand degré d'intermédiarité (38,85). Cela indique que les trois types d'organisations communiquent entre elles par l'entremise de la présidence. L'indice de centralité d'intermédiarité est également élevé pour le Comité national de coordination du renseignement (22,29) et le Centre du renseignement financier (18,17). Bien que le cas du Comité national de coordination du renseignement (NICOC) soit pertinent pour appuyer l'intention de transformer le comité en un lieu majeur de communication entre les nœuds du réseau, le cas du Centre du renseignement financier (FIC) se démarque par le grand nombre de relations informelles qu'il entretient avec d'autres organisations du système de renseignement. Comme nous l'avons observé dans d'autres pays, le dénommé cluster du renseignement financier et fiscal a pris de l'importance et exige des études plus approfondies.

En fait, la distribution du pouvoir dans le système de renseignement national de l'Afrique du Sud penche fortement en faveur du président et de la SSA. Nous y ajoutons l'influence du NICOC et du FIC. Il convient par ailleurs de ne pas sous-estimer l'importance de la SSA dans la configuration actuelle (après 2009) du système de renseignement sud-africain. Cette agence concentre également les services corporatifs (ressources humaines, TI, infrastructure, logistique et finances) qui étaient auparavant redondants dans différentes agences. Elle est également chargée d'assurer l'unité de commandement et la cohérence des objectifs des différentes branches de l'activité de renseignement : l'interne, l'externe et le technique. En raison de la position de la SSA dans le réseau, le président ne subordonne directement aucune agence de renseignement.

Pays	Types d'unité			Indices d'unité				Index de réseau	
	GOV	COO	AGE	Centralités de degrés les plus élevées		Centralités d'intermédiarité les plus élevées		Centralisation des degrés	Centralisation de l'intermédiarité
				Unité	Valeur	Unité	Valeur		
BR	22	05	23	PR	22,38	ABIN	32,38	0,206	0,314
RU	06	0	07	PR	36,84	GRU	30,91	0,364	0,208
IN	07	02	20	PM	14,29	NCTC	20,50	0,116	0,260
CH	10	0	24	MSS	18,52	GSCPC	27,19	0,184	0,428
SA	05	02	11	SSA	20	PR	38,85	0,159	0,394

Tableau 1: Systèmes nationaux de renseignement dans le groupe BRICS

Conclusion

Nous avons essayé de répondre, dans le présent article, à trois questions : 1. Comment les systèmes nationaux de renseignement sont-ils organisés dans les pays BRICS ? 2. Comment le pouvoir est-il réparti entre les différents organismes de chaque système national de renseignement ? 3. Quelles sont les implications d'une distribution donnée du pouvoir sur le risque organisationnel global du système ?

En ce qui concerne la première question, quelques points communs et diverses spécificités ont été observés dans les cas du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud. Par exemple, la Russie et l'Inde ont des agences civiles de renseignement spécialisées dans la collecte et l'analyse de renseignements relatifs aux menaces à la sécurité internationale. Dans le cas de la Chine (MSS) et de l'Afrique du Sud (SSA), les mêmes missions et fonctions sont assurées par des branches spécialisées (bureaux) de grandes organisations. Le Brésil est le seul pays de l'échantillon qui n'a pas de service de renseignement civil majeur axé principalement sur les menaces extérieures. Indépendamment de ces éléments, le nombre total d'organisations participant à chaque système national de renseignement est beaucoup plus élevé au Brésil (50), en Chine (34) et en Inde (29) qu'en Afrique du Sud (18) et en Russie (13).

Ce seul fait ne peut être considéré comme un indicateur de la capacité ou de l'efficacité d'un système de renseignement donné. Ainsi, la Russie est une grande puissance nucléaire dotée d'armes conventionnelles avancées et d'importantes capacités de projection de forces, mais elle ne dispose que de 7 agences de renseignement majeures. Parallèlement, le Brésil, une puissance régionale, compte 23 agences de renseignement. Dans le cas de la Chine et de l'Afrique du Sud, nous maintenons notre décision de considérer les branches spécialisées du MSS et de la SSA comme des agences distinctes à des fins d'analyse. En tout état de cause, l'Inde (20) et la Chine (24) ont un nombre similaire d'agences de renseignement

en dépit de leurs régimes politiques différents. La présence d'organes collégiaux pour coordonner les différentes parties des systèmes nationaux de renseignement est une caractéristique organisationnelle qui semble être associée à une forme polyarchique de gouvernement. Des institutions comme le NICOC (Afrique du Sud), le JIC (Inde) et le Conseil du SISBIN (Brésil) n'ont pas d'équivalents en Russie ou en Chine.

Pour ce qui est de la deuxième question, en utilisant des mesures au niveau des nœuds (organisation) de la centralité des degrés (autorité) et de la centralité d'intermédiarité (information), nous avons été en mesure d'évaluer comment la répartition du pouvoir varie dans les cinq systèmes nationaux de renseignement. Comme le prévoient les théories de l'évolution des systèmes de renseignement, les dirigeants (démocratiques et autres) créent des agences pour accroître les capacités de surveillance de l'état[43]. Ils sont probablement aussi conscients que la création de plusieurs agences permet d'éviter qu'une agence ne devienne trop puissante et n'usurpe le dirigeant[44]. Nous devrions ainsi nous attendre à ce que les dirigeants du gouvernement jouissent de plus de pouvoir que les organismes de renseignement[45]. Quel que soit le type de régime politique (présidentiel, parlementaire ou communiste), les états bien établis se caractérisent par une subordination du renseignement aux autorités politiques. Les présidents ont la plus haute centralité des degrés (autorité) en Russie (36,84) et au Brésil (22,38), tout comme le premier ministre en Inde (14,29). Dans le cas de la Chine et de l'Afrique du Sud, les centralités des degrés les plus élevées sont respectivement celles du MSS (18,52) et de la SSA (20).

Cela ne veut pas dire que les services de renseignement sont impuissants. Leur pouvoir vient de leur contrôle des flux d'informations importants (centralité d'intermédiarité). En outre, une grande partie du pouvoir d'un organisme de renseignement vient de ses liens à un puissant allié au niveau gouvernemental. Nous avons observé cette caractéristique dans le cas de l'ABIN au Brésil, du FSB en Russie, de l'IB et de la RAW en Inde, ou dans les divers bureaux de renseignement du ministère de la Sécurité d'État en Chine. Même la puissante agence de sécurité d'État en Afrique du Sud est subordonnée à un ministère de la Sécurité d'État (le successeur du ministère des Services de renseignement). Chaque fois qu'une agence cherche à concentrer trop de pouvoir, l'autorité politique commence à se mobiliser pour l'éviter, comme nous l'avons observé dans le cas du FSB russe. La centralité d'intermédiarité la plus élevée observée dans les cinq pays étaient celle de l'ABIN au Brésil (32,38), de la GRU en Russie (30,91) et du NCTC en Inde (20,50). Dans le cas de la Chine et de l'Afrique du Sud, les centralités d'intermédiarité les plus élevées sont respectivement celles du SGCPC (27,19) et du président (38,85).

Enfin, nous avons également essayé de comparer les cas—au niveau du graphique—qui concernent le risque organisationnel posé par une répartition particulière du pouvoir. Pour rappel, le risque organisationnel est la probabilité que des vulnérabilités internes ou des menaces externes nuisent au réseau. Nous utilisons la centralisation des degrés pour mesurer la résilience/adaptabilité et la centralisation d'intermédiarité pour mesurer la concentration de l'information. Les indices de centralisation respectifs pour le Brésil (0,206), la Russie (0,364), l'Inde (0,116), la Chine (0,184) et l'Afrique du Sud (0,159) indiquent que la Russie court le plus grand risque d'avoir un système de renseignement moins capable de s'adapter à des circonstances stratégiques changeantes, tout en étant le plus résistant parmi les cinq pays.

Il nous est malheureusement impossible de déterminer, à partir de cet indice, la nature de l'impact que les efforts de réforme du président Poutine auront sur le renseignement russe, ou si la crise ukrainienne induira un quelconque stress institutionnel. De même, les indices de centralisation d'intermédiarité respectifs pour le Brésil (0,314), la Russie (0,208), l'Inde (0,26), la Chine (0,428) et l'Afrique du Sud (0,394) indiquent que la Chine a le risque le plus élevé de voir un acteur isolé (MSS) conserver la plupart des informations, agissant ainsi en tant que gardien du réseau. Bien sûr, l'indice lui-même ne révèle rien sur les intentions supposées ou réelles de la CMC, du président ou du MSS. La répression de la corruption sous l'actuel régime de Xi Jinping mérite toutefois notre attention, du point de vue de l'analyse de réseau.

L'analyse de réseau s'est avérée être une approche utile à la promotion d'un programme de recherche comparative dans le domaine des études du renseignement. Jusqu'à présent, nous avons été en mesure d'offrir une méthode de description systématique des systèmes de renseignement nationaux dans des pays comme le Brésil, la Russie, l'Inde, la Chine et l'Afrique du Sud. Il nous a également été possible d'affirmer, avec une certaine corroboration, l'existence d'une relation de cause à effet entre certains milieux organisationnels et un niveau de risque organisationnel plus ou moins élevé dans le cas des systèmes nationaux de renseignement. Conscients des limites de l'analyse de réseau, les chercheurs continueront d'explorer son potentiel en intégrant notamment davantage de données sur les organismes de contrôle externe dans les branches législative et judiciaire du gouvernement. Forts de nouvelles mesures et de données mises à jour, les résultats présentés dans le présent article pourront faire l'objet d'une interprétation d'autant plus qualitative.

Notes

1. GILL, Peter et PHYTHIAN, Mark, « What is intelligence studies? » *The International Journal of Intelligence, Security, and Public Affairs* 18, n°1, 2016, p. 10 ; LOWENTHAL, Mark M., *Intelligence: from secrets to policy*, sixième édition, Thousand Oaks, États-Unis : CQ Press, 2015, pp. 37-69.

2. AGRELL, Wilhelm et TREVERTON, Gregory F., éd., *National intelligence systems: current research and future prospects*, Cambridge : Cambridge University, 2009, p. 304 ; BORAZ , Steven et BRUNEAU, Thomas , éd. *Reforming intelligence: obstacles to democratic control and effectiveness*, Austin, États-Unis : University of Texas Press, 2007, p. 407 ; DAVIES, Philip H. J, et GUSTAFSON, Kristian C., ed., *Intelligence elsewhere: spies and espionage outside the Anglosphere*, Washington : Georgetown University Press, 2013, p. 256 ; GILL, Peter, « Evaluating intelligence oversight committees: the UK intelligence and security committee and the 'war on terror' », *Intelligence and National Security* 22, n° 1, 2007, pp. 14-37; HASTEDT, Glenn, « Towards the comparative study of intelligence », *Conflict Quarterly* 11, 1991, pp. 55-72 ; HERMAN, Michael, *Intelligence power in peace and war*, Cambridge : Cambridge University Press, 1996, p. 438 ; O'CONNELL, Kevin M., « Thinking about intelligence comparatively », *Brown Journal of World Affairs* 11, n° 1, 2004, pp. 189-199.

3. ANDREGG, Michael M. et GILL, Peter, « Comparing the democratization of intelligence », *Intelligence and National Security* 29, n° 4, 2014, pp. 487-497 ; BORN, Hans et LEIGH, Ian, « Democratic accountability of intelligence services », document stratégique, Genève : Centre de Genève pour le contrôle démocratique des forces armées (DCAF), 2007 ; FARSON, Stuart, GILL, Peter, PHYTHIAN, Mark et SHPIRO, Shlomo, éd., *PSI handbook of global security and intelligence: national approaches*, deux volumes, Westport/Londres : Praeger Publishers, 2008, p. 700 ; LEMOZY, Susana C et SWENSON, Russell G., éd., *Democratization of intelligence: melding strategic intelligence and national discourse*, Washington, DC : National Defense Intelligence College, 2003, p. 127 ; UGARTE, José Manuel, *Legislación de inteligencia*, Buenos Aires : Editorial Dunken, 2001, p. 518.

4. CEPIK, Marco et AMBROS, Christiano, « Intelligence, crisis and democracy: institutional punctuations in Brazil, Colombia, South Africa and India », *Intelligence and National Security* 29, n° 4, 2014, pp. 523-551 ; ESTEVEZ, Eduardo E., « Comparing intelligence democratization in Latin America: Argentina, Peru and Ecuador cases », *Intelligence and National Security* 29, n° 4, 2014, pp. 552-580 ; PHYTHIAN, Mark, « Intelligence theory and theories of international relations: shared world or separate world? » in *Intelligence theory: key questions and debates*, éd. GILL, Peter, MARRIN, Stephen, et PHYTHIAN, Mark, New York : Routledge, 2008, pp. 54-72.

5. Pour une discussion sur la signification et les différentes façons de classer les pays BRICS, voir COOPER, Andre et FLEMES, Daniel, « Foreign policy strategies of emerging powers in a multipolar world: an introductory review », *Third World Quarterly* 34, n° 8, 2013, pp. 943-962 ; HURRELL, Andrew , « Rising powers and the emerging global order », in *The globalization of world politics : an introduction to international relations*, éd. BAYLIS, John, SMITH, Steve et OWENS, Patricia, Oxford : Oxford University Press, 2014, pp. 80-94 ; et VISENTINI, Paulo Fagundes, ADAM, Gabriel, VIERIA, Maíra, SILVA, André, et PEREIRA, Analúcia, *BRICS: as potências emergentes: China, Russia, Índia, Brasil e África do Sul*, Rio de Janeiro : Editora Vozes, 2013, p. 232.

6. ARMSTRONG, Helen, JOHNSON, Anthony, et MCCULLOH, Ian, *Social network analysis with applications*, New Jersey, États-Unis : John Wiley & Sons, 2013, p. 18.

7. Selon l'hypothèse proposée par Cepik et Ambros, l'une des variables qui affectent la capacité d'apprentissage et l'évolution des systèmes nationaux de renseignement est le degré de différenciation fonctionnelle (division du travail) observé dans chaque pays.

8. HANNEMAN, Robert A. et RIDDLE, Mark, *Introduction to social network methods*, Riverside, États-Unis : University of California Press, 2005, p. 60.

9. Les sources spécifiques à chaque pays sont mentionnées tout au long de l'article.

10. ANDREGG et GILL, « Comparing the democratization of intelligence », p. 488.

11. KEEFE, Patrick R., « Privatized spying: the emerging intelligence industry », in *The Oxford handbook of national security intelligence*, éd. JOHNSON, Loch K., Oxford : Oxford University Press, 2010, pp. 296-309.

12. Les graphiques (G) sont des objets abstraits formés par un ensemble V de sommets (ou nœuds) et un ensemble E d'arêtes (ou liens). En d'autres termes, G = (V, E). La théorie des graphes et l'algèbre relationnelle forment la base mathématique du domaine de l'analyse de réseau. Les statistiques et les algorithmes de calcul constituent d'autres fondements méthodologiques importants ; BRANDES, Ulrik et ELERBACH, Thomas, éd, *Network analysis: methodological foundations*, Berlin : Springer, 2005, p. 472.

13. Cf. www.casos.cs.cmu.edu/projects/ora/software.php. D'autres logiciels d'analyse de réseau existent. Voir HUISMAN, Mark et VAN DUIJN, Marijtje A. J., « A reader's guide to social network analysis software », in *The SAGE handbook of social network analysis*, éd. John Scott et Peter J. Carrington, Washington : SAGE Publications Ltd, 2011, pp. 578-597.

14. BRANDES et ERLEBACH, *Network analysis*, pp. 92-95 ; Pour poursuivre la discussion sur l'insuffisance des indices de centralité dans la mesure du pouvoir, voir BORGATTI, Stephen P., « Centrality and network flow », *Social Networks* 27, 2005, pp. 55–71.

15. FREEMAN, Linton C., « Centrality in social networks conceptual clarification », *Social Networks* 1, 1979, pp. 215-239.

16. ARMSTRONG, JOHNSON, et MCCULLOH, *Social network analysis with applications*, p. 320 ; HANNEMAN et RIDDLE, *Introduction to social network methods*.

17. ARMSTRONG, JOHNSON, et MCCULLOH, *Social network analysis with applications*, pp. 205-234.

18. Selon Cepik et Ambros, le risque organisationnel en ce sens est propice aux crises institutionnelles, qui tendent à être plus récurrentes dans le domaine du renseignement que dans d'autres secteurs du gouvernement en raison du secret, de l'absence de contrôles externes appropriés et d'une faible différenciation fonctionnelle.

19. Comme le souligne Russell Swenson (courriel aux auteurs), « une plus grande résilience, sur un plan davantage culturel, pourrait aussi impliquer qu'aucun 'commandant', parmi les membres du système, ne pousse les autres organisations à s'adapter à de nouvelles situations ou menaces. Chaque unité bureaucratique est dès lors encline à maintenir ses vieilles habitudes, même si elles sont moins productives qu'auparavant ».

20. Deux types d'annexes sont consultables sous forme de suppléments en ligne sur le site Web de la Revue brésilienne de science politique. Tout d'abord, des tableaux pour chaque pays détaillant les noms de toutes les organisations, leurs types (gouvernement, coordination, agence) et les valeurs des deux indices (Degré et intermédiarité). Deuxièmement, les graphiques (un pour chaque pays) où les nœuds colorés en rouge représentent les organisations de type 1 (gouvernement), les nœuds colorés en vert les organisations de type 2 (coordination) et les bleus les organisations de type 3 (agences). Bien qu'il ne soit pas possible de visualiser chaque lien individuellement, plus la couleur du bord est foncée, plus la relation d'autorité ou de communication est intense.

21. BRANDÃO, Priscila C., *Serviços secretos e democracia no Cone Sul: premissas para uma convivência legítima, eficiente e profissional*, Niterói; Brésil : Impetus, 2010, p. 302 ; CEPIK, Marco , « Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais », *DADOS* 48, n° 1, 2005, pp. 67-113; CEPIK, Marco, « Structural change and democratic control of intelligence in Brazil », in *Reforming intelligence: obstacles to democratic control and effectiveness*, éd. Thomas Bruneau et Steven Boraz, Austin, États-Unis : University of Texas Press, 2007, pp. 149-169 ; GONCALVES, Joanisval Brito, « The spies who came from the tropics: intelligence services and democracy in Brazil », *Intelligence and National Security* 29, n° 4, 2014, pp. 581-599.

22. CEPIK, Marco, *Espionagem e democracia*, Rio de Janeiro : Editora, 2003, pp. 207-212.

23. Outre la loi 9 883/1999, l'organisation et le fonctionnement du SISBIN sont régis par le décret 4.376/2002. Le décret 8 793/2016 établissant les premières lignes directrices d'une politique nationale du renseignement a finalement été publié (après plus de cinq ans d'attente) par le gouvernement intérimaire Temer en juin 2016, au moment même où une série de procédures de destitution controversées étaient lancées à l'encontre de la présidente élue Dilma Rousseff. Reflétant le besoin de garanties juridiques et de légitimité en période de troubles politiques, la nouvelle politique nationale en matière de renseignement se borne à réitérer la stricte adhésion des activités de renseignement brésiliennes aux principes constitutionnels. Présenté par l'élu Jô Moraes (PCdoB/MG) dans le but de réglementer les procédures opérationnelles de l'ABIN et le contrôle judiciaire de la collecte de renseignements secrets dans le pays, le projet de loi 3 578/2015 devrait avoir des conséquences bien plus positives—s'il parvient à sortir du labyrinthe du Congrès national.

24. Le Bureau du ministère public (MP) est un organe brésilien composé de procureurs indépendants, tant au niveau fédéral (Ministério Público da União) qu'au niveau des états (Ministério Público Estadual). Bien que le rôle joué par certains organismes relevant du MP en matière de renseignement semble s'accroître, ils n'ont pas été inclus dans notre analyse en raison du caractère non officiel de leur appartenance au SISBIN.

25. Le directeur de l'ABIN est un citoyen qui doit se soumettre à des auditions devant le Sénat, tandis que le ministre du Bureau de sécurité institutionnelle (GSI) a été un officier des Forces armées nommé par le Président de la République. Cet arrangement est problématique pour le fonctionnement démocratique du renseignement au

Brésil ; ROTH, Luiz Carlos de Carvalho, « Uti exploratoribus: credibilidade e controle da atividade de inteligência no Brasil », mémoire de Master, Ciência Política, Niterói, Brésil : Universidade Federal Fluminense, 2009.

26. À l'origine, l'ABIN exerçait la fonction de coordination du SISP. L'une des raisons du transfert de responsabilité au SENASP était l'existence de problèmes opérationnels et de litiges entre l'ABIN et le ministère de la Justice. Cependant, le SENASP lui-même se heurte à la résistance de la Police fédérale qui, à son tour, présente des difficultés dans la coopération avec d'autres polices d'État ; CEPIK, Marco, « Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais, » DADOS 48, n° 1, 2005, pp. 67-113.

27. Une constatation qui renforce les études récentes sur le développement des systèmes de renseignement au Brésil se rapporte à la forte centralité d'intermédiarité (7,3) du Centre d'opérations et de gestion du Système de protection de l'Amazonie (CENSIPAM). Créé en 2002, il est axé sur une région critique à la sécurité et au développement du Brésil. Le Centre rassemble les acteurs de différentes parties du système et se concentre sur les résultats, stimulant la coopération inter-agences. Voir MARQUES, Flávio César de Siqueira, « Fusão de dados na inteligência militar », thèse de doctorat, Ciências Militares, Rio de Janeiro : Escola de Comando e Estado Maior do Exército (ECEME), 2016 ; et CERÁVOLO, Túlio Marcos Santos, « A integração da inteligência nas operações interagências no Brasil contemporâneo », mémoire de Master, Ciências Militares, Rio de Janeiro : Escola de Comando e Estado Maior do Exército (ECEME), 2014.

28. GALEOTTI , Mark et SHUMATE, Johnny, *Russian security and paramilitary forces since 1991*, Oxford : Osprey Publishing, 2013, p. 64 ; SOLDATOV, Andrei, « Russia », in *PSI handbook of global security and intelligence: national approaches*, éd. Stuart Farson, Peter Gill, Mark Phythian et Shlomo Shpiro, Westport/Londres : Praeger Publishers, 2008, pp. 479-497.

29. SOLDATOV, « Russia ».

30. Voir aussi le Comité national antiterroriste (NAK), créé en 2006. Il est subordonné au FSB, mais nous n'avons pas pu déterminer s'il a autorité sur d'autres organismes de renseignement. Au sein de la Communauté des États indépendants (CEI), il existe un Centre antiterroriste de la Communauté des États indépendants (CIS ATC), créé en 2000 pour coordonner l'échange d'informations entre les pays membres de l'institution, www.iacis.ru/eng/about/partners/partnerskie_organizatsii/antiterroristicheskiy_tsentr_sng.

31. GALEOTTI et SHUMATE, *Russian security and paramilitary forces since 1991*.

32. CEPIK, Marco, « Segurança nacional e cooperação Sul-Sul: Índia, África do Sul e Brasil », in *Brasil, Índia e África do Sul: desafios e oportunidades para novas parcerias*, éd., Maria Regina Soares de Lima et Monica Hirst, São Paulo, Brésil : Paz e Terra, 2009, pp. 63-118.

33. ASHTANA, N. C. et NIRMAL, Anajali, *Intelligence and security management*, Jaipur, Inde : Pointer Publishers, 2004, p. 454.

34. BANERIJ, Rana, « Legalising intelligence gathering », *The Hindu* 8 juillet 2014, www.thehindu.com/opinion/op-ed/legalising-intelligence-gathering/article6186885.ece?css=print.

35. Créé après les attaques sur le district pakistanais de Kargil dans la région du Ladakh en 1999. Aborde l'évolution des relations indo-pakistanaises depuis 1947, la guerre au Cachemire et la question nucléaire. Le comité a cherché à déterminer si le type d'agression aurait pu être anticipé par les services de renseignement et quels étaient les échecs possibles qui ont permis l'attaque surprise. Mais beaucoup de ces propositions n'ont été mises en œuvre qu'en 2008, après les attentats de Mumbai, dont la paternité fait encore débat ; CEPIK et AMBROS, « Intelligence, crisis and democracy ».

36. VAUGHN, Bruce, « The use and abuse of intelligence services in India », *Intelligence and National Security* 08, n°1, 1993, pp. 01-22.

37. SINGH, V. K., Général de division, *India's external intelligence: secrets of research and analysis wing (RAW)*, New Delhi, Inde : Manas Publications, 2007, pp. 157-170 ; VAUGHN, « The use and abuse of intelligence services in India ».

38. Il s'agit d'une erreur courante commise par des observateurs dont les écrits sont guidés par certaines influences idéologiques. À cet égard, citons l'ouvrage, par ailleurs fort utile, du journaliste français FALIGOT, Roger, *O serviço secreto chinês*, São Paulo, Brésil : Larousse, 2009, p. 543.

39. Pour le contexte général de sécurité, voir le chapitre 18 de KISSINGER, Henry, On China, New York : Penguin Press, 2011, p. 624 ; ainsi que SHAMBAUGH, David, *China goes global: the partial power*, Oxford : Oxford University Press, 2013, p. 432. En ce qui concerne la composante renseignement de la modernisation militaire en Chine, voir BLASKO, Dennis J., *The Chinese army today : tradition and transformation for the 21st Century*, New

York : Routledge, 2006, p. 256; ainsi que CORDESMAN, Anthony H. et KLEIBER, Martin, *Chinese military modernization: force development and strategic capabilities*, Washington : CSIS, 2007, p. 226.

40. Après avoir pris en considération leurs missions spécifiques, leurs exigences techniques, leurs dimensions organisationnelles et le nombre de personnes employées, nous avons pris la décision analytique de prendre en considération 12 bureaux spécifiques sous l'autorité du ministère de la Sécurité de l'État (MSS) comme des agences de renseignement distinctes. Dans le cas contraire, le nombre total d'agences de renseignement en Chine passerait de 24 à 12. Voir GUO, Xuezhi, *China's security state: philosophy, evolution, politics*, Cambridge : Cambridge University Press, 2012, p. 496.

41. Le Projet Avani était une opération de renseignement destinée à évaluer l'impact de la bataille de succession présidentielle de l'ANC sur la stabilité du pays. Dans le cadre de ce projet, la NIA a intercepté des courriels de personnes occupant des postes supérieurs, qui auraient conspiré pour empêcher Zuma de devenir président de l'ANC. L'inspecteur général a conclu que les courriels étaient faux et a recommandé des mesures disciplinaires contre les responsables. Le directeur de la NIA à l'époque (Masetlha) a été démis de ses fonctions par le président Mbeki, ainsi que par deux officiers supérieurs ; O'BRIEN, Kevin, « Controlling the hydra : a historical analysis of South African intelligence accountability », in Who's watching the spies ? Establishing intelligence service accountability, éd. Hans Born, Genève : Centre pour le contrôle démocratique des forces armées (DCAF), 2005), pp. 199-222.

42. CEPIK AND AMBROS, « Intelligence, crisis and democracy », pp. 541-545.

43. BAYLEY, David H., « The police and political development in Europe », in *The formation of national states in Western Europe*, éd. Charles Tilly, Princeton, États-Unis : Princeton University Press, 1975, pp. 328-379 ; CEPIK, *Espionagem e democracia* ; TILLY, Charles, *Coerção, capital e estados europeus: 1990-1992*, São Paulo, Brésil : EdUSP, 1996, p. 356.

44. Russell Swenson a attiré notre attention (courriel aux auteurs) sur l'importante motivation des dirigeants à concevoir des systèmes de renseignement composé de plus d'une agence. Voir GILL, Peter, *Policing politics: security intelligence and the liberal democratic state*, Ne : York: Routledge, 1994, p. 384 ; de même que MATEI, Florina Cristiana, et BRUNEAU, Thomas, « Intelligence reform in new democracies: factors supporting or arresting progress », *Democratization* 18, n° 3, 2011, Pp. 602-630. Pour des exemples historiques de systèmes de renseignement et de sécurité devenus à ce point puissant qu'ils ont usurpé le pouvoir en formant un état policier, voir le SNI au Brésil et le BOSS en Afrique du Sud.

45. Pour une théorie institutionnaliste du développement des systèmes de renseignement, voir ZEGART, Amy B., *Flawed by design : the evolution of the CIA, JCS, and NSC*, Stanford, États-Unis : Stanford University Press, 1999, p. 336. Les approches fondées sur le pouvoir et les approches institutionnelles en matière de sécurité nationale ne s'excluent pas mutuellement.