Existe-t-il un cyberespace centrasiatique ?

dimanche 31 mars 2019, par Grégory JOUBERT

L'annonce de la mise en retrait relatif du président Noursoultan Nazarbaïev, le 19 mars 2019, a attiré l'attention sur le Kazakhstan, ex-république soviétique d'Asie centrale de 2,7 millions de km2 (18,4 millions d'habitants). L'occasion de se poser une question : existe-t-il un cyberespace centrasiatique ? La première partie de cette étude solidement documentée a pour principal objectif de traiter de la dépendance infrastructurelle des États d'Asie centrale à la Russie. Sur la base de ces considérations, une deuxième partie présente le vecteur d'influence que constitue le cyberespace, ainsi que de la perception que se fait le pouvoir kazakhstanais de ce terrain conceptuel. De l'influence informationnelle subie à l'absence de prise en compte de l'aspect profondément technique du cyberespace, le Kazakhstan est foncièrement un État vulnérable. Dans la troisième partie, Grégory Joubert se penche plus particulièrement sur les leviers d'action utilisés par les autorités pour le contrôle des activités de la population en ligne et les moyens de surveillance dont dispose le pays. Outre son intérêt propre, cette étude peut aussi être féconde pour réfléchir aux relations entre les pays de l'Union européenne et une autre puissance de l'Internet, les Etats-Unis.

ESPACE devenu incontournable pour la réflexion militaire, le cyberespace revêt désormais une dimension stratégique inscrite dans les doctrines des principales puissances de la planète. Composés d'infrastructures physiques, logiques et informationnelles, ses réseaux deviennent à bien des égards de redoutables vecteurs d'influence et sont aujourd'hui au centre de nombreuses polémiques au retentissement international. Dans le cas de la Russie plus particulièrement, on observe une multiplication des accusations liées au cyberespace. Du pirate informatique supposément soutenu par les services de sécurité de la Fédération à ses tentaculaires organes médiatiques, l'influence prêtée aux réseaux russes dans de nombreuses crises politiques contemporaines est devenue un thème récurrent dans les débats occidentaux.

Dans ce nouvel espace de rivalités de pouvoir, les espaces aux marges de la Fédération de Russie se révèlent être des territoires pertinents à analyser. Pour ces États indépendants enclavés, aux infrastructures de communication entièrement dépendantes du centre moscovite sous l'Union soviétique, les conditions ne semblent pas avoir fondamentalement changé depuis 1991, date de la fin de l'URSS. La situation de ces anciennes périphéries coloniales dans le domaine du cyberespace est aujourd'hui marquée par des logiques d'influence et de coercition, dans la continuité de ce passé. Une analyse en est ici proposée.

Existe-t-il un cyberespace centrasiatique ?

La présente étude s'intéresse de manière plus appuyée au Kazakhstan et se compose de trois parties. La première a pour principal objectif de traiter de la dépendance infrastructurelle des États de la région à la Russie. Sur la base de ces considérations techniques, une deuxième partie traite du vecteur d'influence que constitue le cyberespace, ainsi que de la perception que se fait le pouvoir kazakhstanais de ce terrain conceptuel. De l'influence informationnelle subie à l'absence de prise en compte de l'aspect profondément technique du cyberespace, le Kazakhstan est foncièrement un État vulnérable en de nombreux points. Dans la troisième partie, nous nous intéressons plus particulièrement aux leviers d'action utilisés par les autorités pour le contrôle des activités de la population en ligne et aux moyens de surveillance dont dispose le pays.

I. Dans le cyberespace : une influence structurelle de la Russie sur ses anciens satellites

Le développement des infrastructures

Qu'il soit question des infrastructures routières, ferroviaires, des flux migratoires, financiers ou culturels, la Russie reste aujourd'hui la seule voie de transit de flux fiable à laquelle les acteurs de la région peuvent recourir. Cette situation d'enclavement et de permanence des voies de communications dirigées vers le Nord se traduit également dans le champ du cyberespace. L'analyse cartographique de ces territoires composés de câbles et de routeurs interconnectés permet de restituer l'organisation des voies de télécommunications, dont le développement nécessite investissements massifs et coopération entre les acteurs en assurant la gouvernance.

La première dorsale transnationale connectant la région, le *Trans Asie-Europe* (TAE) développé en 1998, a, dès sa mise en service, présenté des problèmes structurels. Si les États ont dès lors été connectés aux réseaux mondiaux au moyen de cette nouvelle artère, le fait est que la structuration du cyberespace repose foncièrement sur des logiques économiques et politiques. Ses capacités de transit de données limitées (622ms/s) en font une dorsale où l'offre est inférieure à la demande, rendant son coût d'utilisation élevé. De plus, le trop grand nombre d'acteurs (publics et privés) de nationalités différentes impliqués dans la gouvernance de la dorsale TAE la rend par nature inefficiente. Le réseau fonctionne comme un « patchwork de câbles nationaux », à la gestion d'ensemble incohérente [1].

La connectivité des États de la région ne s'est réellement développée qu'au rythme des projets émanant de la Russie. Le réseau *Trans Europe-Asie* (TEA) développé en 1999 relie le centre névralgique de l'Internet européen (Francfort) à Hong Kong, en longeant le parcours du Transsibérien [2]. Chemin le plus court pour la transmission de données entre ses deux extrémités, cette dorsale permet également de pallier une congestion des câbles à Suez (Egypte). Son développement a été permis par la prise de participation d'opérateurs européens, russes et chinois. Ses ramifications sur les territoires centrasiatiques ont quant à eux été rendus possibles par les opérateurs russes, *Rostelecom* et *TransTelecom*, en direction du seul territoire de la région frontalier de la Russie, à savoir le Kazakhstan.

Les réseaux russes représentent dès lors les voies privilégiées pour la transmission de données. Leur large bande passante, mais également le nombre restreint d'accords nécessaires pour le transit de données, en sont les principaux arguments techniques.

L'analyse des Systèmes Autonomes (*Autonomous* System ; AS) traduit la place centrale qu'occupe la Russie dans les flux de télécommunications [3]. S'il existe des interconnexions avec les réseaux chinois avec des capacités de bande passante connectées importantes, ces dernières ne sont pourtant, à l'hiver 2018, que peu sollicitées. Aussi, les jonctions de câbles chinois et centrasiatiques semblent surtout être utilisées pour les flux financiers, les Systèmes Autonomes qui y sont reliés étant principalement des institutions bancaires. Les opérateurs du TAE ne sont en revanche pas sollicités par les réseaux centrasiatiques. Ce qui démontre la faible centralité de cette dorsale.

Cette situation tient également à l'histoire. Au-delà du fait que la connectivité de la région ait principalement dépendu des projets russes sur le plan technique, le partage d'une langue et d'une culture commune en est un autre facteur déterminant.

Le *Runet* : un vecteur de puissance

L'utilisation préférentielle de réseaux de télécommunication orientés vers la Russie tient également aux plateformes d'intermédiation utilisées par la population de la région. *Yandex*, *Vkontakte*, *Mail.ru* sont les composantes principales du *Runet*, l'Internet russophone [4]. Comparables dans leur fonctionnement aux GAFAM (*Google, Apple, Facebook, Amazon, Microsoft*) américains ou aux BATX chinois (*Baidu, Alibaba, Tencent, Xiaomi*), elles brassent un nombre considérable de données, stockées et traitées dans des centres de données localisés en Russie. L'utilisation préférentielle des réseaux de télécommunication en direction de la Russie tient également, dès lors, à l'utilisation de ces plateformes dont les ressources se retrouvent sur son territoire.

La réalité de ces pratiques sur Internet n'est pas sans conséquences. Sur la base du traitement des données qui sont ainsi produites, c'est toute une économie qui se développe. Le pouvoir politique n'est pas en reste puisque ces données sont également à la disposition des services de renseignements russes, qui peuvent y accéder sans réelles contraintes [5] grâce à la législation.

Par la possession de sa propre industrie numérique, la Russie est théoriquement dans la capacité d'imposer à ses opérateurs de stocker les données que ceux-ci traitent sur son territoire [6]. Les États d'Asie centrale ne possédant ni ce type d'industrie, ni les capacités de stockage conséquentes, n'ont alors que peu de marge de manœuvre quant au destin des données produites par leur population.

Les autorités peuvent tout au plus demander que les données produites par leurs citoyens soient stockées sur leur territoire ou, à défaut, bloquer la ressource. Les autorités kazakhstanaises ont déjà émis ce type de demande auprès de Google, qui a répondu par une fin de non-recevoir. Au mois de juin 2011, l'entreprise américaine a même décidé de rediriger pendant deux semaines les requêtes provenant de google.kz vers google.com, donc vers un système algorithmique relié aux requêtes mondiales et non plus nationales [7].

Induite par la géographie (physique) et les usages de la population, la faiblesse infrastructurelle des pays de la région les pousse indubitablement dans une situation de dépendance structurelle vis-à-vis de la Russie. De plus, cette dernière affiche une recherche de développement de son influence. Le projet de *datacenter* d'Omsk répond à cette volonté d'accaparement des données. Directement relié par câbles de fibre optique, il permettra aux opérateurs russes d'offrir un temps de latence moindre pour le transfert de données, mais également de mettre en valeur de nouveaux territoires répondant à des considérations (cyber)stratégiques plus larges encore [8].

Les intérêts politiques et économiques liés aux données produites sont conséquents. Le Kazakhstan, s'il souhaite effectivement mener une politique souveraine sur ses données, n'aura d'autre possibilité que de se placer dans une position offensive à l'égard de la Russie. Au vu de leur importance, le déni d'accès aux plateformes russes sur l'ensemble du territoire serait une décision lourde de conséquences. Le principal dilemme que poserait un blocage de ressources de grande ampleur est que ces plateformes sont d'une utilité précieuse pour les services de renseignements et de police. Même s'il paraît convenable de douter des capacités techniques d'interception réelles dont disposent les autorités, l'analyse de données ouvertes (comme les commentaires sur des articles en ligne) permet, en soi, de bénéficier d'une image du ressenti de la population sur les politiques menées. Elle permet également de contrôler de possibles messages dissidents ou appels à manifestation pouvant y circuler et d'arrêter les auteurs de ces derniers.

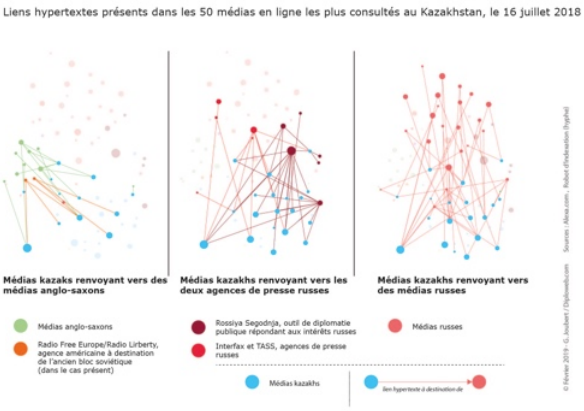
II. Le Kazakhstan : une puissance régionale vulnérable…

Une influence informationnel russe

Au-delà d'une dépendance aux infrastructures et plateformes d'intermédiation russes, l'influence du Nord sur la couche sémantique, sur l'information, en est un prolongement logique. Si la Russie ne peut être

considérée comme un modèle vertueux quant à la pratique du journalisme, le traitement de l'information demeure néanmoins de meilleure qualité par rapport à ce qui prévaut dans la région [9]. Dans le cas du Kazakhstan, un contrôle étatique fort rend peu crédibles pour une large partie de la population kazakhe des supports nationaux manquant de réelles analyses portant sur les problèmes ayant cours à l'intérieur du territoire.

La formation des journalistes tient également un rôle important quant au poids de la Russie dans l'information. Les formations en kazakh ou en russe ne laissent que peu de place à l'apprentissage d'autres langues, comme l'anglais. Bien que des universités proposent des formations coûteuses en anglais, cet argument n'est que commercial, le russe prédominant au sein de celles-ci. Du fait de ces faiblesses en langues, les sources utilisées par les journalistes kazakhs, notamment concernant l'information internationale, proviennent principalement de médias russophones.



Le schéma ci-dessus, effectué à l'aide du robot d'indexation hyphe du Medialab de l'Institut d'Etudes Politiques de Paris, représente tous les liens hypertextes présents sur les principaux sites d'information kazakhs. De celui-ci, réalisé le 16 juillet 2018, lendemain de la finale de la coupe du monde et jour de la rencontre entre MM. Donald Trump et Vladimir Poutine à Helsinki, il ressort une très faible utilisation de sources non-russes. L'analyse de certains articles révèle même des copies conformes d'articles produits au sein de rédactions basées sur le territoire de la Fédération de Russie.

Bénéficiant d'une audience majoritaire au Kazakhstan, y compris en dehors de ses relais spécialement à destination de l'étranger, le pouvoir russe possède dès lors un puissant vecteur d'influence. L'absence de réels débats dans l'espace médiatique kazakhstanais fait que la population est bien mieux informée sur les questions touchant la Russie qu'à propos de son propre pays. Les débats centrés sur celle-ci, au sein des organes télévisuels notamment, confèrent à ceux ayant trait au Kazakhstan (peu nombreux) un caractère exceptionnel et une force de frappe proportionnellement décuplée.

Cette influence certaine est de plus intégrée par les médias russes, qui s'en sont notamment servi après l'abstention du Kazakhstan sur une résolution du Conseil de Sécurité de l'ONU du 14 avril 2018 condamnant les actions de la coalition occidentale en Syrie. A la suite de cette prise de position, lors du talk-show « *Dimanche soir avec Vladimir Soloviev* », deuxième programme le plus regardé en Russie, ce dernier s'est interrogé sur cette abstention, ainsi que sur le passage du Kazakhstan à l'alphabet latin. La perspective d'un « Maïdan » [10] au Kazakhstan fut même posée en direct [11]. Les semaines suivantes ont vu fleurir sur Internet divers articles faisant état d'une coopération militaire entre le Kazakhstan et les États-Unis sur la mer Caspienne. Bien qu'il s'agisse de fausses informations déjà relayées par le passé, la coopération entre les deux États ne concernant que le fret non-militaire, les autorités kazakhes ont été contraintes de s'exprimer à plusieurs reprises pour rétablir la réalité des faits.

Même si des réflexions s'engagent sur la prééminence des médias d'information au Kazakhstan, la relation entre les autorités kazakhstanaises et les ressources informationnelles russes révèle aussi une certaine proximité. Lors de manifestations, comme celles ayant eu lieu en 2016 contre la prolongation de la durée de location des terres agricoles de dix à vingt-cinq ans, seuls les sites d'informations occidentaux,

comme *Azattyq*, ont été bloqués. Ce dernier est l'un des rares médias traitant en profondeur des problèmes affectant le Kazakhstan, et qui en donne des analyses. Ainsi, si lors de ces manifestations, *Azattyq* publia plusieurs articles sur le sujet, son homologue russe Sputniknews(.kz) ne fit que des résumés des événements, et se garda d'analyser plus profondément les problèmes profonds gangrénant la société kazakhstanaise. Les médias russes dans leur ensemble n'ont fait qu'évoquer ces événements. Ce comportement rédactionnel dénote une proximité des vues dans le traitement des soulèvements entre le pouvoir kazakhstanais et son voisin, ce dernier n'interférant que lorsque ses propres intérêts sont en jeu, mais avec une force de frappe à même de sérieusement déstabiliser son voisin.

Une faible prise en compte des problèmes infrastructurels

Dans la conception russe, le terme *d'espace informationnel* prévaut sur celui de cyberespace. Ce terme vise à prendre en compte les multiples aspects composants le cyberespace, y compris ses aspects cybernétiques, tout en gardant comme finalité stratégique la protection première de l'information et son contrôle. Dans ce cadre, les réseaux numériques, et en premier lieu Internet, sont considérés comme étant des vecteurs d'informations sur lesquels la souveraineté de l'État doit s'établir au même titre que pour tout média de masse, et sont donc sujets à régulation [12]. Cette notion d'espace informationnel prévaut également au Kazakhstan.

Néanmoins, l'interprétation kazakhstanaise de celle-ci souffre de défauts conceptuels. Les mesures prises par les autorités jusqu'en 2017 à ce sujet portaient quasi-exclusivement sur la couche sémantique du cyberespace. Les mesures prises pour sa protection n'ont pas pris en considération l'aspect profondément technique et infrastructurel que revêt pourtant le contrôle de l'information. Dans son acception kazakhstanaise, la notion d'information a longtemps été simplement considérée sous ses aspects médiatiques.

Découlant de cette interprétation littérale, les lacunes dans le domaine de la cybersécurité sont conséquentes et les exemples de déficiences nombreux – d'agents des services de sécurité intérieure (le KNB) minant de la cryptomonnaie *via* les serveurs d'infrastructures critiques, au piratage du site Internet du Ministère de la Défense, en passant par la compromission des serveurs du Ministère des Affaires Intérieures par un adolescent qui avait suivi pas à pas un tutoriel sur Internet ; ceux-ci ne donnent pas lieu à contre-offensive. Au 6 juin 2018, selon le système de monitoring développé par le centre d'analyse et d'investigation des cyberattaques (*Tsarka*), sur les 495 sites du domaine gouvernemental kazakhstanais (.gov.kz), seuls 55 ont un protocole SSL valide. Le protocole SSL est pourtant le protocole garant de la sécurité et de la confidentialité des informations qui transitent entre l'utilisateur du site Internet et les serveurs de ce dernier. Ajoutons qu'à la même date deux sites du domaine étaient défacés [13], 8 « infectés » et 98 étaient indisponibles. Ces informations ne sont désormais plus publiées publiquement.

Approuvé le 28 octobre 2017 par le président Noursoultan Nazarbaïev, le projet de *cyber-bouclier* [14], dont l'avancée notable serait une prise en considération de l'aspect cybernétique du cyberespace, laisse sceptiques les spécialistes de terrain. La rédaction de ce projet a été l'objet d'amers débats entre la principale organisation indépendante de cybersécurité du pays et les Services Techniques de l'État, laissant transparaître le manque de volonté de ces derniers sur le sujet.

L'un des exemples les plus révélateurs de cette prise de distance des autorités concerne l'intégration de mesures statistique de l'avancement des actions entreprises dans ce cadre sur la base de standards internationaux. La prise en considération de l'indice de cybersécurité du *Global Cybersecurity Index*, publié chaque année par l'Union Internationale des Télécommunications, n'a été intégrée dans le projet de cyber-bouclier qu'après deux jours de discussions. Et pour cause, cet indice permet une comparaison avec les autres pays. D'après Olzhas Satiev (co-fondateur de l'organisation de cybersécurité Tsarka), la difficile intégration de cette mesure tient à la difficulté de modifier l'indice, notamment de le fausser. Or, il s'agit là d'une pratique relativement courante au sein des administrations du pays, à des fins de communication publique. Au total, il semble que la mise en place de cet outil de suivi sera laborieuse. La dernière vulnérabilité critique en date fut publiée sur la page Facebook du groupe Tsarka le 8 février 2019 [15]. Alors que ses membres avaient notifié aux autorités des vulnérabilités permettant l'accès à

toutes les informations internes à l'ambassade de la république du Kazakhstan en Russie (y compris les mots de passe des administrateurs) dix jours auparavant, celles-ci n'avaient toujours pas été corrigées et avaient même été aggravées.

L'exil des spécialistes vers des contrées aux salaires valorisants, l'absence de formation à la « bonne hygiène numérique » des corps administratifs, la cupidité de certains fonctionnaires, l'inaction des Services Techniques de l'État : rien ne prédispose à un environnement numérique sécurisé dans le pays. Les orientations politiques dans ce domaine restent cantonnées à un rapport coût/bénéfice à court-terme. Le chantier de la sécurisation des réseaux, conséquent et nécessitant un effort de longue haleine, est dès lors occulté dans la pratique.

III. … aux capacités limitées

Le blocage de ressources : premier levier d'action dans « l'espace informationnel »

En dépit du manque de prise en compte de déficiences techniques pourtant considérables, les autorités kazakhes sont néanmoins volontaires sur des aspects plus visibles d'Internet. Dérivant du développement de la conception d'*espace informationnel*, la priorité donnée à l'information visible et compréhensible par tous a poussé les organes de sécurité à se développer sur ce terrain, dans une volonté d'en assurer un contrôle répondant à des intérêts de court-terme.

Le prolongement de l'action étatique dans le champ du cyberespace est un corollaire logique du contrôle de l'information au sein de toutes les rédactions. À la suite des émeutes ayant eu cours dans la cité pétrolière de Zhanaozen en 2011, qui ont fait émerger un nouveau médium d'information (les blogueurs) [16], tout l'arsenal législatif relatif à l'information en ligne a été profondément remodelé.

La mesure la plus usitée par les autorités consiste à interdire l'accès aux ressources en ligne qu'elles mettent sur la sellette. Les motifs d'interdiction d'accès sont nombreux et assez flous pour pouvoir englober tous types de contenus : de la pédopornographie à l'opposition politique (extrémisme-séparatisme-terrorisme) [17]. C'est ainsi que, lors de chaque intervention de la principale figure d'opposition Mukhtar Ablyazov, exilé en France, tous les contenus photographiques et vidéos publiés à son sujet sont inaccessibles sur les réseaux sociaux au Kazakhstan. Son parti politique « Choix Démocratique du Kazakhstan » est considéré depuis mars 2018 comme extrémiste, ce qui fait que toute publication le soutenant est sujette à blocage (réalisé par les Services Techniques de l'État, ainsi que par le KNB), les auteurs s'exposant de leur côté à des poursuites.

Depuis 2016, les contenus peuvent ainsi être bloqués sur Internet, sur simple ordre extrajudiciaire et sans justification, par les services de sécurités kazakhstanais et les ministères. Ces opérations sont automatisées, et peuvent donc être réalisées à grande échelle.

Des interceptions aux intrusions : un marché globalisé

Le renseignement dans la sphère des données numériques et le contrôle des contenus sont permis à grande échelle au moyen de la technologie russe SORM (Sistema Operativno-Rozysknykh Meropriyatiy ou Système des Activités de Recherche Opérationnelles). Sa troisième version inclut la technologie dite du *Deep Packet Inspection* (DPI). Son fonctionnement consiste en un déploiement de nœuds d'interceptions au sein desquels transitent tous les réseaux de télécommunications, directement reliés aux locaux des services de l'État. Les fournisseurs d'accès à Internet opérant au Kazakhstan sont dans l'obligation d'installer le système sur leurs réseaux. De plus, pour les connexions vers l'étranger, tous les opérateurs dans le domaine des télécommunications sont dans l'obligation de se connecter aux réseaux de l'opérateur national Kazakhtelecom. Depuis le mois de mai 2018, ils sont également dans l'obligation légale de stocker sur le territoire du Kazakhstan les données de leurs utilisateurs, ainsi que les métadonnées produites par ces derniers (protocole utilisé, date et heure d'inscription dans le réseau, IP, temps passé en

ligne, IP de la ressource Internet).

Traiter des technologies d'interception reste chose complexe. Un état des lieux de la situation dans les pays centrasiatiques dans ce domaine a été réalisé par Privacy International en novembre 2014 [18]. Faire l'analogie entre les marchés des interceptions / intrusions et ceux de l'armement semble pertinent, tant les uns comme les autres répondent à des objectifs étatiques, avec implication d'acteurs privés, dans des secteurs remarqués pour leur opacité.

La standardisation autour de SORM permet avant tout la mise en place de coopérations entre les États de la région et la Russie dans le domaine sécuritaire. La normalisation des pratiques et technologies utilisées est en cours, dans le cadre des diverses structures, principalement la Communauté des États Indépendants (CEI) et l'Organisation du Traité de Sécurité Collective (OTSC), toujours orientées sur la « sécurité de l'information ». Dans le cadre d'exercices communs entre membres de l'OTSC, il n'a pas été question de contrer d'éventuelles intrusions sur les systèmes mais plutôt d'analyser et de bloquer les ressources jugées extrémistes. La traduction dans le champ technique de ces accords interétatiques passés dans les domaines du renseignement est difficile à mesurer, mais la normalisation des pratiques ne peut indéniablement être impulsée que par la Russie… qui possède la majorité des données produites par la population centrasiatique, et bénéficie de fait des ressources pour l'analyse de ces données. Si la technologie du DPI permet de collecter un nombre conséquent de données, d'autres technologies sont nécessaires pour surveiller les réseaux, nécessitant d'autres fournisseurs spécialisés. Si la technologie russe d'analyse sémantique de l'activité sur les réseaux existe et s'exporte (par MFI-Soft au Kazakhstan et en Ouzbékistan), encore faut-il avoir accès aux contenus. En ce sens, autant la loi obligeant les fournisseurs d'accès Internet au sein des États peut être mise en place, autant seul un nombre limité de données peuvent être récupérées, obligeant nécessairement à coopérer avec la Russie dans ces domaines.

La position de la Russie dans la sphère du cyberespace vis-à-vis des États centrasiatique est dès lors intégrée dans une logique de domination. Alors que Russie et Chine, deux « puissances cyber », ont été signataires d'accords bilatéraux de coopération et de non-agression en 2015 [19], aucun accord de ce type n'a été passé avec les acteurs de la région. Plus encore, l'utilisation de l'espace informationnel (et de manière plus générale du cyberespace dans son ensemble) fait partie de l'arsenal coercitif dont dispose la Russie afin de défendre ses intérêts, et sa remise en cause ne semble pas être à l'ordre du jour.

Néanmoins, la Russie n'est pas le seul exportateur dans la région. Bien que la standardisation du renseignement soit opérée autour de SORM, la surveillance des réseaux a été confiée, dans les cas du Kazakhstan et de l'Ouzbékistan, à deux sociétés israéliennes, Nice Systems et Verint Systems.

Se basant sur SORM, ces dernières permettent, en plus des métadonnées, l'analyse des SMS, MMS, publications sur les forums ainsi que la reconnaissance vocale et faciale des contenus transitant sur les nœuds du système. Les technologies de ces sociétés ayant leurs centres à Astana, Almaty et Tachkent, y sont trois fois plus chères que leurs substituts russes, préférés par les services kirghizes. L'utilisation préférentielle de solutions israéliennes, au-delà de leur aspect qualitatif prouvé, peut être interprété comme une volonté de l'Ouzbékistan et du Kazakhstan de garder une marge de manœuvre au niveau de leur appareil sécuritaire.

L'utilisation de technologies étrangères est particulièrement avérée dans le domaine des interceptions ciblées permettant de capter notamment des informations jusqu'alors inaccessibles par les services de renseignements de la région (comme des données issues de Facebook ou Whatsapp, pour ne citer qu'eux). Il s'agit de produits coûteux dont le champ est plus limité que celui de SORM puisqu'il est question, dans le cas de ce type d'activités, d'intrusions sur les appareils de personnes ciblées précisément. Le spectre de celles-ci indique toutefois que l'attention portée par les services reste politiquement motivée, et dépasse le simple cadre anti extrémisme-terrorisme-séparatisme. Les outils de communication de Mukhtar Ablyazov et de sa famille ont ainsi été interceptés et contrôlés grâce à l'implication de l'entreprise italienne Hacking Team [20]. L'ont été également des organisations féministes au Kazakhstan, dans des proportions difficilement quantifiables. Néanmoins, des conversations privées de leurs membres sur Whatsapp ont été interceptées par le KNB local, et des pressions effectuées grâce à ces dernières [21].

L'utilisation de spywares (logiciels espions) a été rapportée par l'Electronic Frontier Foundation. Plus particulièrement, le logiciel Finfisher a été fourni par les entreprises anglaise Gamma et suisse Dreamlab aux autorités kazakhes et ouzbèkes. L'entreprise israélienne NSO group a également vendu au Kazakhstan le logiciel d'intrusion Pegasus. Mais de nombreux autres contrats avec d'autres entreprises ont été passés, pour des services dont les capacités réelles sont difficiles à établir.

*

Le *Kaznet*, une chimère ?

Utilisant à l'intérieur de ses frontières le terme de *Kaznet* pour en définir son espace informationnel, le cyberespace kazakh ne revêt pour autant aucun élément permettant de conclure une quelconque position d'indépendance ou de supériorité pouvant être pris en compte dans des logiques de rapports de force. La dépendance accrue de la région vis-à-vis de la Russie, tant par ses aspects infrastructurels qu'informationnels, peut même en quelque sorte laisser transparaître un processus de colonisation numérique. L'extraction des données de la région et leurs traitement et valorisation sur le territoire de la Russie, qui dispose des capacités idoines, ne laisse à ces États que peu de marge de manœuvre pour leur contrôle.

La focalisation sur l'information, au détriment de la protection des infrastructures critiques ou contenant les données de leurs citoyens en font des États vulnérables, potentiellement faciles à déstabiliser par d'autres qui bénéficient de capacités offensives dans le champ du cyberespace. La collaboration sécuritaire des États de la région avec la Russie dans le cadre de la CEI et de l'OTSC (à laquelle l'Ouzbékistan et le Turkménistan ne sont néanmoins pas associés) ne laisse pour le moment pas apparaître une quelconque coopération dans le domaine de la cybersécurité sur un plan technique. La permanence au sein de ces structures de la domination par la Russie, qui a par le passé manipulé la menace sécuritaire posée notamment par le Mouvement Islamiste d'Ouzbékistan pour répondre à ses propres intérêts, laisse penser que les mêmes mécanismes sont à l'œuvre en 2019. La protection des infrastructures cybernétiques dans la région par le biais d'une collaboration, et donc d'un échange de capacités dans ce domaine, ne va pas dans le sens des intérêts de la Russie, dont le potentiel offensif résulte en partie de l'existence de vulnérabilités sur les systèmes physiques de ses alliés et adversaires.

De même, les relations de la région avec la Chine, peu évoquées dans la présente étude, ne se traduisent en 2019 que dans le domaine sécuritaire, dans les sphères informationnelles. La principale coopération revient à de l'échange d'informations dans le cadre de l'Organisation de la Coopération de Shanghai, à vocation sécuritaire. L'écosystème numérique fermé du voisin chinois en fait un acteur informationnel à l'influence faible dans la région. Aussi, même si le pendant « digital » du projet *Belt and Road Initiative* fait état de volontés de prises de positions dans les affaires des pays dans la région, l'efficience de ces projets ne sera véritablement mesurable que lorsque ces derniers seront plus avancés. Toutefois, par les investissements massifs qui y sont opérés, notamment dans le domaine des transports, il parait très probable que la Chine aura la volonté de protéger ses acquis. Il en sera nécessairement de même avec les projets émanant des « routes de la Soie digitales » dont l'opacité est constante.

La coopération sino-russe, partageant une conception similaire du cyberespace sera dès lors à analyser dans ses prolongements qui auront immanquablement lieu, et dont la région dépend. Alors que les positions russes dans le domaine économique tendent à être concurrencées par celles de la Chine, celles dans les domaines sécuritaires, et notamment dans le cyberespace, sont un champ au sein duquel se retranscriront nécessairement des prises de position par les deux puissances dans le futur. En tout état de cause, peu laisse à penser qu'un cyberespace centrasiatique avec sa propre identité soit à même d'émerger.

Le *Diploweb.com* s'attache à vous en offrir les clés de l'Asie, avec des documents inédits rédigés par des experts, diplomates, universitaires, stratèges. **Diploweb publie à votre intention ce livre : Pierre Verluise (dir.), « *Histoire, Géographie et Géopolitique de l'Asie. Les dessous des cartes, enjeux et rapports de forces* », éd. Diploweb, via Amazon**

P.-S.

Grégory Joubert est en deuxième année de Master à l'Institut Français de Géopolitique (IFG, Université Paris VIII Vincennes – Saint-Denis) ainsi qu'à l'Université d'Etat pour les Sciences Humaines de Moscou (RGGU). Ses travaux portent sur les stratégies de contrôle dans le champ du cyberespace en Russie et dans les espaces post-soviétiques.

Notes

[1] UNESCAP/ TERRABIT CONSULTING, « In-depth study of broadband infrastructure in North and Central Asia », 2014.

[2] Limonier, Kévin. « Le cyberespace, nouveau lieu d'affirmation de la puissance russe », in RAVIOT, Jean-Robert (dir.), Russie : vers une nouvelle guerre froide, La Documentation Française, Paris, 2016, p.136.

[3] L'interconnexion des réseaux, à la base d'Internet (composante la plus visible du cyberespace), repose sur ces derniers. D'un point A à un point B, la donnée, pour aller à destination, transite par des Systèmes Autonomes connectés entre eux au moyen d'accords commerciaux (appelés protocole BGP ; Border Gateway Protocol).

[4] Limonier, Kévin. « La Russie dans le cyberespace : représentations et enjeux », Hérodote 2014/1 (n° 152-153), p. 140-160. DOI 10.3917/her.152.0140 .

[5] Borogan, Irina & Soldatov, Andrei. « Russian surveillance state », World Policy, 12 septembre 2013, http:// www.worldpolicy.org/journal/fall2013/Russia-surveillance .

[6] « Loi fédérale russe N 242-FZ sur la protection des données personnelles des ressortissants russes », Cil.cnrs. http://www.cil.cnrs.fr/CIL/spip.php?article2751 .

[7] « Google.kz est revenu au Kazakhstan ». Tengrinews. https://tengrinews.kz/internet/Googlekz-vernulsya-v-kazahstan-190571/

[8] Douzet, Frédérick et al., « Les nouveaux territoires stratégiques du cyberespace : le cas de la Russie », Stratégique 2017/4 (N° 117), p. 169-186

[9] Reporter sans Frontières, https://rsf.org/fr/classement#

[10] NDLR : Maïdan, référence au mouvement politique ukrainien de 2013-2014.

[11] « Soloviev a attaqué le Kazakhstan ». Novaïa Gazeta, https://www.novayagazeta.ru/articles/2018/04/17/76217-soloviev-napal-na-kazahstan

[12] Limonier, Kévin. « La Russie dans le cyberespace : représentations et enjeux », Hérodote 2014/1

(n° 152-153), p. 140-160. DOI 10.3917/her.152.0140

[13] Le défacement consiste en un piratage informatique dont le résultat se traduit par la modification de la présentation du site Internet ciblé.

[14] Gussarova, Anna. « Kazakhstan Launches 'Cyber Shield' Concept », The Jamestown Foundation, 20 novembre 2017, https://jamestown.org/program/kazakhstan-launches-cyber-shield-concept/

[15] https://www.facebook.com/cyberseckz/

[16] Beisembayeva, Dila. « Exploring the impact of online political activism on political processes in Kazakhstan : the Zhanaozen uprising ». Master of International Communication, Unitec Institute of Technology, 2016, New Zealand.

[17] Freedom House, « Freedom on the Net », https://freedomhouse.org.

[18] Privacy International, « Private interests : monitoring Central Asia », novembre 2014, https://privacyinternational.org/report/837/private-interests-monitoring-central-asia

[19] « Have Russia and China signed a cyber nonaggression pact ? », The Diplomat, https://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/

[20] Electronic Frontier Foundation, « Operation Manul », https://www.eff.org/fr/wp/operation-manul

[21] Entretien mené avec le groupe féministe Feminita à Almaty en mars 2018