

COMMERCE

La Route de la soie numérique, le nouveau péril chinois?



La Chine veut exporter son modèle autoritaire de gestion de l'internet. Plusieurs pays affiliés au projet Belt and Road y ont déjà souscrit



Julie Zaugg, Hong Kong



L'initiative Belt and Road (BRI) comporte une face moins visible: la constitution d'une route de la soie numérique. En Chine, les internautes sont cantonnés derrière un «mur de feu» qui les empêche d'accéder aux contenus que l'Etat n'approuve pas. Leurs propos sont aussi soumis à la censure et ils font l'objet d'une surveillance serrée, grâce à des outils technologiques comme la reconnaissance faciale. «La Chine cherche désormais à exporter ce modèle de cybercontrôle autoritaire», juge Stewart Patrick, du groupe de réflexion Council on Foreign Relations.

Cette route de la soie numérique passe en premier lieu par la construction de réseaux de fibre optique sur le territoire des pays ayant rejoint l'initiative. Les groupes chinois Huawei, ZTE, China Telecom, China Unicom et China Mobile ont obtenu des contrats pour en bâtir en Birmanie, au Bangladesh, au Cambodge, au Kirghizistan, au Népal, en Ouganda et en Equateur. Au Pakistan, Huawei a récemment inauguré un réseau de 820 kilomètres à Islamabad, pour un coût de 44 millions de dollars, dont les 85% avaient été fournis par Exim Bank of China, une institution affiliée à l'Etat.

Lire également: Guerre technologique: la Chine a plus à perdre que les Etats-Unis

Plusieurs entreprises de tech chinoises ont en outre conclu des partenariats avec des organes de l'Etat, comme la Chinese Association for Friendship, subordonnée au Ministère des affaires civiles, afin d'écouler leurs produits dans les pays affiliés à la BRI. C'est notamment le cas de Venustech et de DBAPP Security, deux groupes de cybersécurité, indique Kieran Green, un expert des affaires sécuritaires de la Chine. Cloudwalk, une firme basée à Pékin, a de son côté conclu un contrat avec le Zimbabwe pour lui fournir ses solutions de reconnaissance faciale. Son homologue Yitu vend les siennes à la police malaisienne.

Lire aussi l'opinion: En finir avec la peur de l'hégémonie chinoise

Des séances d'entraînement

A cela s'ajoute une série de séminaires et séances d'entraînement organisés par la Chine pour ses partenaires au sein de la BRI. Un forum sur la cybersécurité organisé à Zhangjiajie en octobre 2018 a réuni plus de 500 représentants de pays affiliés à l'initiative. L'armée du Sri Lanka, des journalistes thaïlandais, philippins et arabes, ainsi qu'une délégation vénézuélienne ont tous bénéficié de formations sur la gestion de leurs réseaux internet, indique l'ONG Freedom House dans un rapport.

Et un billet d'opinion: Cinquante nuances de Chine

Certains, à l'instar du Vietnam, de la Thaïlande et de l'Ouganda, ont par la suite adopté des lois sur la cybersécurité qui imitent de près la législation en vigueur dans l'Empire du Milieu. La Russie s'est elle aussi inspirée du «mur de feu» chinois.

Risque de fuites de données

Cette route de la soie numérique soulève des questions sur le plan sécuritaire. «L'intégration de logiciels de cybersécurité dans l'infrastructure d'autres pays facilite les activités d'espionnage des services secrets chinois», estime Kieran Green. Notamment grâce à l'introduction de portes dérobées leur permettant d'accéder à des données normalement confidentielles. De même, «celui qui installe un câble de fibre optique peut y insérer des micro-ondulations», souligne Stewart Patrick. Cela permet de générer des fuites de données pouvant être captées par un récepteur.»