diploweb.com La revue géopolitique
ISSN : 2111-4307

La recherche d’une souveraineté numérique en Russie : à qui profite-t-elle ?

dimanche 13 juin 2021,par Marie-Gabrielle BERTRAN

Citer cet article / To cite this version :
Marie-Gabrielle BERTRAN, **La recherche d’une souveraineté numérique en Russie : à qui profite-t-elle ?** , *Diploweb.com : la revue géopolitique, 13 juin 2021.*

Les liens entre le secteur privé et les institutions publiques dans le domaine du numérique en Russie sont le témoignage des nouvelles logiques de cyberdéfense du pays. En effet, ils concourent à la construction d'une souveraineté numérique russe, en partie destinée à protéger ses réseaux. Mais ils sont aussi le signe de l'influence majeure de certains acteurs privés sur les autorités, via, notamment, un rôle de conseil décisif dans l'établissement des nouvelles législations et doctrines sur le numérique en Russie.

Contexte et enjeux : l'émergence du concept de souveraineté numérique (« *tsifrovoj suverenitet* ») en Russie

LE PROBLEME de la sécurité des systèmes d'information est pris en compte par les autorités russes depuis les années 1990 au moins. En 1998, la délégation russe à l'Assemblée Générale des Nations Unies a prôné la mise en place d'une première résolution sur les « Évolutions dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale » (*Résolution A/RES/53/70*) [1]. Cette demande de prise en considération des risques cyber au niveau international est intervenue un an avant la découverte de l'opération « *Moonlight Maze* », la cyberattaque la plus importante de l'histoire des États-Unis jusqu'à la découverte de la compromission du logiciel « *SolarWinds* » en 2020.

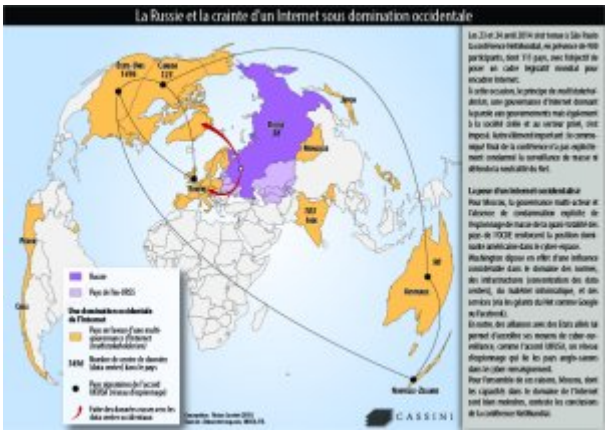
Lancée en octobre 1996, l'opération « *Moonlight Maze* » avait consisté en des intrusions répétées dans des systèmes informatiques militaires aux États-Unis, pour répondre à des objectifs de renseignement militaro-stratégiques. Ces intrusions avaient été perpétrées par des pirates informatiques qui utilisaient les réseaux de Fournisseurs d'accès à l'Internet (F.A.I.) russes, tels que Cityline, et un code informatique qui comprenait des éléments en cyrillique. À l'aide de ces indices, un groupe d'enquête du « *Federal Bureau of Investigation* » (F.B.I.) s'était rendu en Russie, et avait eu la confirmation qu'il s'agissait d'une opération menée par les services de renseignement russes eux-mêmes.

Dans le cadre de la Guerre froide (1947-1991), les agences de sécurité russes prenaient déjà en compte, par ailleurs, la présence possible de portes-dérobées (« *backdoors* ») dans du matériel informatique et des logiciels provenant de l'étranger. La possibilité qu'une entreprise ou un État insère volontairement des failles exploitables dans des logiciels exportés vers d'autres pays était donc déjà envisagée par ces services. Les limitations en matière d'importation des technologies visaient notamment à prévenir et à réduire ce risque. Conscient de la persistance de cette problématique malgré la fin de la Guerre froide, le Ministère russe des Affaires Étrangères a établi en 2000 un nouveau Concept de Sécurité Nationale [2] qui prenait en compte le domaine cyber [3]. Selon ce « concept », « [il existait] des menaces croissantes envers la sécurité nationale [russe] dans la sphère informationnelle » [4], due aux efforts de « certains pays pour dominer l'espace informationnel mondial et pour exclure la Russie du marché de l'information sur son territoire et à l'extérieur. » [5]

Selon le Ministère, ce « sérieux danger » avait pour origine « l'élaboration […] d'un concept de guerre informationnelle [6] [par un certain nombre d'États], qui envisageait la création de dangereux moyens d'influence dans les espaces informationnels [7] d'autres pays […] ; tels que

la perturbation du fonctionnement normal des systèmes d'information et de communication, de la fiabilité des systèmes de stockage des sources d'information, et tels que l'obtention illégale ou clandestine d'un accès à ces systèmes. » [8]. La présidence de Dmitrij Medvedev, entre 2008 et 2012, a cependant relégué ces questions de sécurité au second plan et mis en avant l'économie et l'industrie russes du numérique, afin d'attirer les investisseurs en promouvant l'image d'un secteur dynamique et diversifié.

Mais les révélations faites par Edward Snowden [9] à la fin de l'année 2013 ont remis la question de la cyber-sécurité au centre des préoccupations des autorités en Russie. Vingt-deux ans après la chute de l'Union Soviétique et la fin de la Guerre Froide, ces révélations ont vivement rappelé en effet les risques liés à l'emploi de logiciels et d'applications produits par des entreprises soumises à des législations étrangères, et possiblement porteurs de portes-dérobées exploitables par des services de renseignement ou des groupes sponsorisés par des États. La volonté d'assurer la *souveraineté numérique* de la Russie a alors émergé chez différents acteurs publics et privés (centres de recherche, entreprises du numérique), suivant l'idée que la préservation de la sécurité des systèmes d'information du pays ne pourrait se faire que par l'emploi de solutions conçues en Russie. En accord avec cette idée, les autorités russes ont décidé de favoriser l'industrie domestique du numérique, et adopté des mesures en ce sens.



Carte. La Russie et la crainte d'un Internet sous domination occidentale
Cliquer sur la vignette pour agrandir la carte. Conception : F. Carrelet pour Cassini/Diploweb.com (2015)

Leur nouvelle posture en faveur d'un numérique souverain en Russie trouve aujourd'hui son point culminant dans l'élaboration d'un projet de « *RuNet* [10] souverain », qui vise à construire un réseau entièrement indépendant du réseau internet mondial sur l'ensemble de sa structure (depuis la couche matérielle du réseau jusqu'à sa couche applicative, suivant le modèle OSI). De cela résulte une véritable stratégie de *russification* des logiciels et de l'ensemble des applications informatiques qui sont employés en Russie. Conscients des nouvelles opportunités qui leurs sont offertes dans ce cadre, les acteurs du numérique russes (du secteur privé en particulier) se sont emparés de la question. Les nouveaux enjeux de sécurité des infrastructures informatiques de l'État leur ont en effet ouvert un marché intérieur important, alors que le secteur était auparavant négligé par les politiques publiques (à la différence du secteur de l'énergie en particulier).

Ce constat amène à se demander *qui* des autorités ou du secteur privé joue un rôle

véritablement décisif dans la mise en place des nouvelles politiques en faveur d'un numérique souverain en Russie ? Considérons successivement l'influence actuelle de l'idée de cyber-souveraineté en Russie (I) puis les relations entre le secteur public et le secteur privé dans le domaine du numérique en Russie et les enjeux géopolitiques de ces relations (II).

I. L'influence actuelle de l'idée de cyber-souveraineté en Russie

Que signifie l'idée de cyber-souveraineté en Russie, et quel rôle joue-t-elle dans les relations entre les entreprises russes et l'État ? Selon les spécialistes russes de la question [11], le concept de cyber-souveraineté, ou souveraineté numérique en russe (« *cifrovoj suverenitet* ») provient de l'idée française de *souveraineté* développée par Jean Bodin (philosophe, théoricien des lois) au XVIe siècle. Cette idée renvoie au principe de la priorité du gouvernement de l'État [12] sur son territoire : l'État étant alors considéré comme le seul garant légitime de l'intégrité de ce territoire. Ce principe implique que les autorités étatiques puissent mettre en place et faire appliquer différentes mesures, dans tous les domaines qui peuvent être considérés comme fondamentaux pour la stabilité et la sécurité de l'État (économie, éducation, etc.) sur le territoire qu'il organise. Ces mesures peuvent alors être considérées comme relevant de ses prérogatives, mais aussi comme étant des fonctions obligatoires du gouvernement de l'État. L'évolution de cette idée a conduit à la définition, au XVIIe siècle, des droits régaliens, puis des fonctions régaliennes [13].

Cependant, le développement des réseaux numériques et de l'Internet entre les années 1970 et 2000 [14], implique que différents acteurs puissent attaquer à distance des infrastructures qui peuvent être considérées comme critiques pour le fonctionnement et la stabilité des États (usines, centrales électriques, réseaux de communication etc.). Par ailleurs, l'information se propage rapidement et ne peut plus être régulée grâce aux moyens de contrôle historiques, tels que le contrôle des frontières nationales d'un territoire [15]. Or, la volonté de contrôler et d'unifier un vaste territoire composé de populations diverses est un élément constitutif de la construction historique de la Fédération de Russie. La diffusion incontrôlée de l'information (les textes officiels russes parlent souvent de « dissémination de l'information », « *rasprostranenie informacii* »), et l'accroissement de la vulnérabilité des réseaux sont donc perçus par les autorités russes comme une menace fondamentale pour la souveraineté et à la stabilité de la société et de l'État.

Après les révélations d'Edward Snowden, le gouvernement russe entendait donc contrôler le développement de l'industrie numérique en Russie, et éduquer la population russe aux problématiques de sécurité informationnelle qui pouvaient la concerner (sécurité des données personnelles, opérations d'influence d'autres États sur les réseaux sociaux, etc.).Cette volonté a conduit à la mise en place d'un « Plan pour le développement d'une société de l'information en Russie 2011-2020 », remanié en 2017 pour la période 2017-2030. La mise en œuvre de ces plans repose en grande partie sur l'implication du secteur privé du numérique russe, dont les solutions sont cruciales pour la souveraineté numérique du pays. Cet état de fait amène à s'interroger sur les relations entre les secteurs public et privé dans ce domaine.

II. Les relations entre le secteur public et le secteur privé dans le domaine du numérique en Russie et les enjeux géopolitiques de ces relations

Les premières entreprises du secteur des technologies à avoir établi les pratiques *marketing* et les règles du marché international dans le domaine du numérique sont celles qui ont été créées aux États-Unis au début des années 1980, avec l'émergence du marché des machines individuelles (« *Personal Computers* » (PCs) et MacIntosh).

En comparaison, les entreprises russes ont eu une présence plus tardive et restreinte sur le marché international, dont elles maîtrisaient moins bien les codes. Cette présence tardive et limitée a conduit au développement d'un fort tropisme national de ces entreprises, qui s'insèrent avec plus de facilité sur le marché russophone [16]. Cette focalisation des acteurs privés russes sur leur marché intérieur les a ainsi amenés à nouer des relations étroites avec les acteurs publics, en particulier depuis 2010 et le mandat présidentiel de Dmitrij Medvedev.

Une démarcation s'est alors établie entre les acteurs qui profitent de leurs relations au point de devenir assez solides pour pouvoir se projeter sur le marché international, et les autres. De grands groupes ont ainsi émergé au début des années 2000, tels que Mail.ru (« *Mail.Ru Group* »), qui a peu à peu racheté les solutions russophones les plus utilisées sur les marchés russe et post-soviétique. Son vaste écosystème de solutions comprend un service de messagerie *e-mail* Mail.ru, des réseaux sociaux (VK, OK.ru et My World), des messageries instantanées (Agent et ICQ), une plateforme de jeux en ligne [17] et de communication (My.com), des moteurs de recherche, de e-commerce et une plateforme de recrutement (Search, Headhunter, Price comparison), un service de *cloud* [18], ainsi qu'un service d'investissement et de capital-risque, DST Global. C'est via cette plateforme d'investissement dirigée par Jurij Mil'ner que le groupe parvient à rayonner à l'international.

En 2009, DST Global a réalisé d'importants investissements dans Twitter et Facebook, via un montage complexe qui permettait de dissimuler l'origine russe des investisseurs, et de contourner les éventuelles limitations qui pouvaient leur être imposées, voire les éventuels refus qui pouvaient leur être opposés par les organismes financiers étatsuniens. Twitter et Facebook peuvent être considérées en effet comme des entreprises stratégiques, puisque leur modèle d'affaires repose sur la circulation de l'information et les données personnelles des utilisateurs de leurs solutions. Ce statut stratégique implique donc une vigilance accrue des autorités étatsuniennes vis-à-vis de l'origine et de la provenance des investissements qui y sont injectés. DST Global (Hong-Kong) a donc investi dans Twitter et Facebook via DST USA II et DST Investments 3. Ces investissements ont atteint plusieurs millions de dollars. **En 2010, DST contrôlait ainsi jusqu'à 8 % des parts de Facebook et 5 % des parts de Twitter.**

Les acteurs privés du secteur du numérique jouent donc un rôle de plus en plus important auprès des autorités en Russie, qui s'en servent notamment pour réaliser des prises stratégiques sur le marché international des technologies. Mais elles les consultent également afin d'orienter leurs décisions en matière de législation du numérique. Ces acteurs ont donc un impact direct sur la manière dont évoluent la perception et le rôle du numérique en Russie. Cette influence apparaît par exemple à travers le rôle politique de l'oligarque Igor Achmanov, principal détenteur du groupe de sécurité informatique InfoWatch. Igor Achmanov est, en

effet, l'un des principaux instigateurs de la doctrine de souveraineté numérique qui est actuellement mise en œuvre en Russie, dans les domaines de l'économique et de l'industrie. Il a directement participé, par ailleurs, à la définition et à la mise en place d'une nouvelle doctrine sur la sécurité de l'information en 2016, en tant que conseiller auprès de la présidence. L'influence des acteurs privés est également visible à travers les marques de reconnaissance publiques qui leur sont témoignées. Le 26 août 2020, un décret présidentiel (*ukaz* n°529) a ainsi été adopté pour la décoration officielle de deux entrepreneurs, Natal'ja Kasperskaja (directrice générale d'InfoWatch, ex-épouse d'Eugène Kaspersky et actuelle compagne d'Igor Achmanov) et Artemij Lebedev, pour leur rôle actif dans le développement d'un Internet russe souverain.

Ces liens entre le secteur privé et les institutions publiques dans le domaine du numérique en Russie sont donc le témoignage des nouvelles logiques de cyberdéfense du pays, **puisqu'ils concourent à la construction d'une souveraineté numérique russe, en partie destinée à protéger ses réseaux. Mais ils sont aussi le signe de l'influence majeure de certains acteurs privés sur les autorités, via, notamment, un rôle de conseil décisif dans l'établissement des nouvelles législations et doctrines sur le numérique en Russie**.

*****

À première vue, les nouvelles logiques de cyber-souveraineté et de *russification* des logiciels qui sont employés en Russie favorisent l'émergence d'une industrie dynamique et de confiance. Cette industrie est composée d'acteurs qui sont prêts non seulement à suivre, mais aussi à promouvoir la mise en œuvre des nouvelles orientations publiques en matière de souveraineté numérique, puisqu'elles sont directement en accord avec leurs intérêts propres. Cette nouvelle dynamique est d'ailleurs également à l'origine de certains abus de la part des acteurs privés. Certaines entreprises utilisent en effet l'idée de *souveraineté numérique* uniquement comme un outil *marketing*, dans le but de vendre leurs solutions aux institutions publiques.

L'entreprise Elvis Neotekh, une filiale de RosNano, a ainsi vendu des milliers de caméras de sécurité au Ministère russe de l'Éducation nationale, en arguant que ces caméras fonctionnaient grâce à un logiciel russe. Cependant, un audit mené par un spécialiste à l'été 2020 a démontré que ces caméras utilisaient un micrologiciel (« *firmware* ») chinois, qui comportait plusieurs failles de sécurité, dont une porte-dérobée [19]. Il était donc possible de contrôler ces caméras à distance et en temps réel, de capter leur flux vidéo, ou de s'en servir comme de composants d'un « *botnet* », afin de miner des cryptomonnaies, ou encore de mener des attaques par déni de service distribué (*DDoS*) depuis le territoire russe.

Bonus vidéo. La bataille de l'Internet : Etats-Unis /

Russie, un point partout ?

En 2017, Laurent Bloch et Kevin Limonier, experts d'Internet, répondent en vidéo aux questions du *Diploweb.com*. Clair et pédagogique. Très utile pour comprendre cette nouvelle dimension de la conquête de la puissance. (8 minutes)

Plus

Découvrez la Masterclass Diploweb : Pourquoi les données numériques sont-elles géopolitiques ?

La numérisation de pans entiers de l'activité humaine est aujourd'hui une évidence. De moins en moins d'actes du quotidien échappent aux réseaux sur lesquels on les pratique, a fortiori en temps de pandémie : passer un coup de fil à des proches, suivre un cours, se déplacer dans la rue avec un smartphone … Toutes ces activités anodines génèrent des données numériques qui font l'objet de bien des convoitises, qu'elles soient commerciales, politiques ou stratégiques.

Parce qu'elles circulent à la surface du globe via un maillage complexe de câbles, de protocoles et de plateformes, **nos données sont géopolitiques.** A la fois objet et source de pouvoir, elles sont au cœur d'un nombre croissant de conflits, tandis que plus aucune guerre n'échappe au numérique. C'est d'ailleurs cette réalité qui est au centre du concept de Datasphère.

Pourquoi les données numériques sont-elles géopolitiques ? MasterClass de Kevin Limonier

L'objectif de **ce cours de Kevin Limonier** est donc de comprendre les enjeux géopolitiques inhérents à cette datasphère dans laquelle nous évoluons toutes et tous. Loin d'être déconnectée du monde physique, elle en est plutôt un prolongement – comme une sorte de réalité augmentée que nous autres géographes commençons à peine à explorer.

Bibliographie

ASSEMBLEE GENERALE DES NATIONS UNIES, « Developments in the Field of Information and Telecommunications in the Context of International Security », 4 janvier 1999. URL : https://undocs.org/A/RES/53/70 [voir la version française au lien suivant : https://undocs.org/fr/A/RES/53/70].

DOUZET, Frédérick, DESFORGES, Alix, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 21 décembre 2018. URL : http://journals.openedition.org/netcom/3419 .

BOYER, Bertrand, *Guérilla 2.0, Guerres irrégulières dans le cyberespace*, préface du général d'armée Thierry Burkhard, éditions de l'École De Guerre, collection « Ligne De Front », 2020.

GERASIMOV, Oleg, « Comment une filiale de Rosnano a vendu, avec l'aide de Rostekh, des milliers de caméras « russes » à des écoles avec un micrologiciel chinois vérolé » (« Kak dočka Rosnano, prodavšaja s Rostekhom tysjači kamer v školy, delaet « rossijskie » kamery s dyrjavoj kitajskoj prošivkoj »), Habr.com, 20 juin 2020. URL : https://habr.com/ru/post/507498/.

KUCERIAVYJ, Mikhajl Mikhajlovič, « Société de l'information mondialisée et problèmes de sécurité » (« Global'noe informacionnoe obščestvo i problemy bezopasnosti »), Communication et Société (*Kommunikacij i obščestvo*), septembre 2013, p. 90-92.

MINISTERE DES AFFAIRES ÉTRANGERES DE LA FEDERATION DE RUSSIE, « Concept de sécurité nationale de la Fédération de Russie », 10 janvier 2000.
URLs :
https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=fr_FR et
https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU [en russe].

P.-S.

Marie-Gabrielle Bertran est doctorante en géopolitique au centre GEODE (Géopolitique de la Datasphère) et à l'Institut français de géopolitique (IFG), rattaché à l'Université Paris 8. Ses recherches portent sur les enjeux du développement logiciel en Russie et sur les relations entre ses différents acteurs (ingénieurs, entreprises et État).

Notes

[1] . « Developments in the Field of Information and Telecommunications in the Context of International Security », résolution adoptée par les Nations Unies le 4 janvier 1999, https://undocs.org/A/RES/53/70.

[2] . Ministère des Affaires Étrangères de la Fédération de Russie, « Concept de sécurité nationale de la Fédération de Russie », III. Menaces pour la sécurité nationale de la Fédération de Russie, 10 janvier 2000, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=fr_FR . Voir https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU pour le texte original en russe. (Le texte présenté ici n'est pas une traduction officielle, mais une traduction de l'auteur).

[3] . Domaine des systèmes d'information numériques, qui comprend l'informatique au sens large (matériel et code informatiques, infrastructures etc.), l'information qui circule en ligne, et les problématiques de sécurité et de défense qui les concernent.

[4] . Ou *datasphère*. Voir Frédérick Douzet et Alix Desforges, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 21 décembre 2018, http://journals.openedition.org/netcom/3419 . « *Usilivajucja ugrozy nacional'noj bezopasnosti Rossijskoj Federacii v informacionnoj sfere*. », Ministère des Affaires Étrangères de la Fédération de Russie, *art. cit.*.

[5] . « *Ser'ëznuju opasnost' predstavljajut soboj stremlenie rjada stran k dominirovaniju v mirovom informacionnom prostranstve, vytesneniju Rossii s vnešnego i vnutrennego informacionnogo rynka* », *Ibid.*.

[6] . Ou guerre de l'information.

[7] . Littéralement, « sur les sphères informationnelles », « *na informatsionnye sfery* », *Ibid.*.

[8] . « *Ser'ëznuju opasnost' predstavljajut soboj […] razrabotka rjadom gosudarstv koncepcii informacionnykh vojn, predusmatrivajuščej sozdanie sredstv opasnogo vozdejstvija na informacionnye sfery drugikh stran mira ; narušenie normal'nogo funkcionirovanija informacionnykh i telekommunikacionnykh sistem, a takže sokhrannosti informacionnykh resursov, polučenie nesankcionirovannogo dostupa k nim.* », *Ibid.*.

[9] NDLR : *France Culture* le présente ainsi : « En 2013, âgé alors de 29 ans, Edouard Snowden, ancien employé de la CIA et de la NSA, permettait au monde entier de découvrir avec quel entrain les agences de renseignement américaines et leurs partenaires s'adonnaient à la surveillance de masse. »

[10] . *Russian interNet* ou *Russian Network*.

[11] . Dont Mikhajl Mikhajlovič Kučeriavyj, Docteur en Sciences Politiques, lieutenant général, directeur du Service Fédéral de Contrôle des Technologies et des Exportations à Saint-Pétersbourg. Mikhajl Mikhajlovič Kučeriavyj, « Société de l'information mondialisée et problèmes de sécurité », *Communication et Société*, septembre 2013, p. 90-92.

[12] . Ou du système de gouvernance de l'État.

[13] . Dans le cadre d'une forme de gouvernement républicaine et démocratique, ce principe persiste, à la seule différence que l'État correspond alors à la société des citoyens qui le compose (notamment par le biais du système représentatif) et qu'il gouverne, suivant une certaine réciprocité.

[14] . Pour ce qui est du réseau de masse à l'échelle mondiale.

[15] . Voir Bertrand Boyer, *Guérilla 2.0, Guerres irrégulières dans le cyberespace*, préface du général d'armée Thierry Burkhard, éditions de l'École De Guerre, collection « Ligne De Front », 2020.

[16] . Qui comprend la Russie et l'espace post-soviétique.

[17] . Jeux sur mobiles et jeux multi-utilisateurs en ligne (MMORPG etc.).

[18] . Service de stockage de données pour PCs et mobiles.

[19] . Oleg Gerasimov, « Comment une filiale de Rosnano a vendu, avec l'aide de Rostekh, des milliers de caméras « russes » à des écoles avec un micrologiciel chinois vérolé », Habr.com, 20 juin 2020, https://habr.com/ru/post/507498/.