Le Grand Firewall de Chine

Architecture d'un État-censeur

Stéphane Fosse
https://fosse.fr

03 mars 2026

Résumé

Le Grand Firewall de Chine n'est pas un pare-feu. C'est une infrastructure d'État à deux couches, opérationnelle depuis 2003, qui filtre en temps réel la totalité du trafic internet entrant et sortant d'un pays de 1,4 milliard d'habitants. Conçue par Fang Binxing, ancien président de l'Université des postes et télécommunications de Pékin, cette architecture a été construite pour durer — et pour s'exporter.

Comment fonctionne techniquement le Grand Firewall de Chine ?

L'internet est arrivé en Chine en 1994. Deux ans plus tard, en 1996, le gouvernement posait les premiers jalons de ce qui allait devenir le système de censure le plus sophistiqué jamais construit. Le Projet Bouclier d'Or (*Golden Shield Project*), officiellement baptisé Projet national de construction d'infrastructure de sécurité des réseaux publics, démarre en 1998 sous l'égide du ministère de la Sécurité publique. Sa première phase, conduite de 1998 à 2006, établit les trois niveaux d'infrastructure réseau et les bases de données partagées. La seconde phase, achevée en 2008, renforce les applications de sécurité publique et étend le dispositif aux provinces centrales et occidentales du pays.

L'architecture repose sur deux couches distinctes. La couche haute concentre quelques opérateurs étatiques qui contrôlent les passerelles internationales : China Telecom, China Unicom, China Mobile, plus trois opérateurs à vocation spécifique (recherche scientifique, éducation, commerce international). Ces nœuds centraux sont les seuls points de connexion entre le réseau chinois et l'internet mondial. C'est là que sont déployés les routeurs équipés de systèmes de détection d'intrusion et d'inspection profonde de paquets (*Deep Packet Inspection*, DPI). La couche basse oblige tous les fournisseurs d'accès à internet locaux à installer des équipements de filtrage certifiés pour obtenir leurs licences d'exploitation.

Les techniques de filtrage se sont stratifiées au fil des années. La première génération bloquait les noms de domaine et les adresses IP directement. La deuxième couche a introduit le filtrage par mots-clés : si une connexion TCP contient des termes politiquement sensibles — « Dalaï-Lama », « Tiananmen », « indépendance du Tibet » — la connexion est réinitialisée par injection de paquets TCP RST. L'empoisonnement DNS (*DNS poisoning*) redirige les requêtes vers des adresses incorrectes. Le blocage d'URL permet de cibler des pages précises sans bloquer un domaine entier. Les entreprises Cisco Systems et Sun Microsystems ont fourni les premiers équipements de censure lors de la construction initiale du dispositif, selon Jyh-An Lee, juriste à l'Université chinoise de Hong Kong [9].

Facebook a été bloqué en 2008. Twitter en 2009. Google, après avoir refusé de laisser le gouvernement contrôler ses serveurs à Pékin, a été bloqué en 2010. Instagram en 2014. YouTube, WhatsApp, Wikipedia, le *New York Times*, *Reporters sans frontières* et des dizaines de milliers d'autres sites suivent la même logique : une liste noire opaque, jamais publiée, mise à jour en continu. Quand un internaute chinois tente d'accéder à un site bloqué, il voit simplement un message d'erreur technique.

Comment le Grand Firewall détecte-t-il le trafic chiffré et les outils de contournement ?

Le vrai défi pour les architectes du système n'est pas de bloquer Facebook — c'est d'empêcher les utilisateurs d'accéder à Facebook malgré le blocage. Dès la troisième phase de développement, le Grand Firewall a été adapté pour détecter les protocoles VPN courants comme IPSec, L2TP/IPSec et PPTP, qui utilisent des ports spécifiques

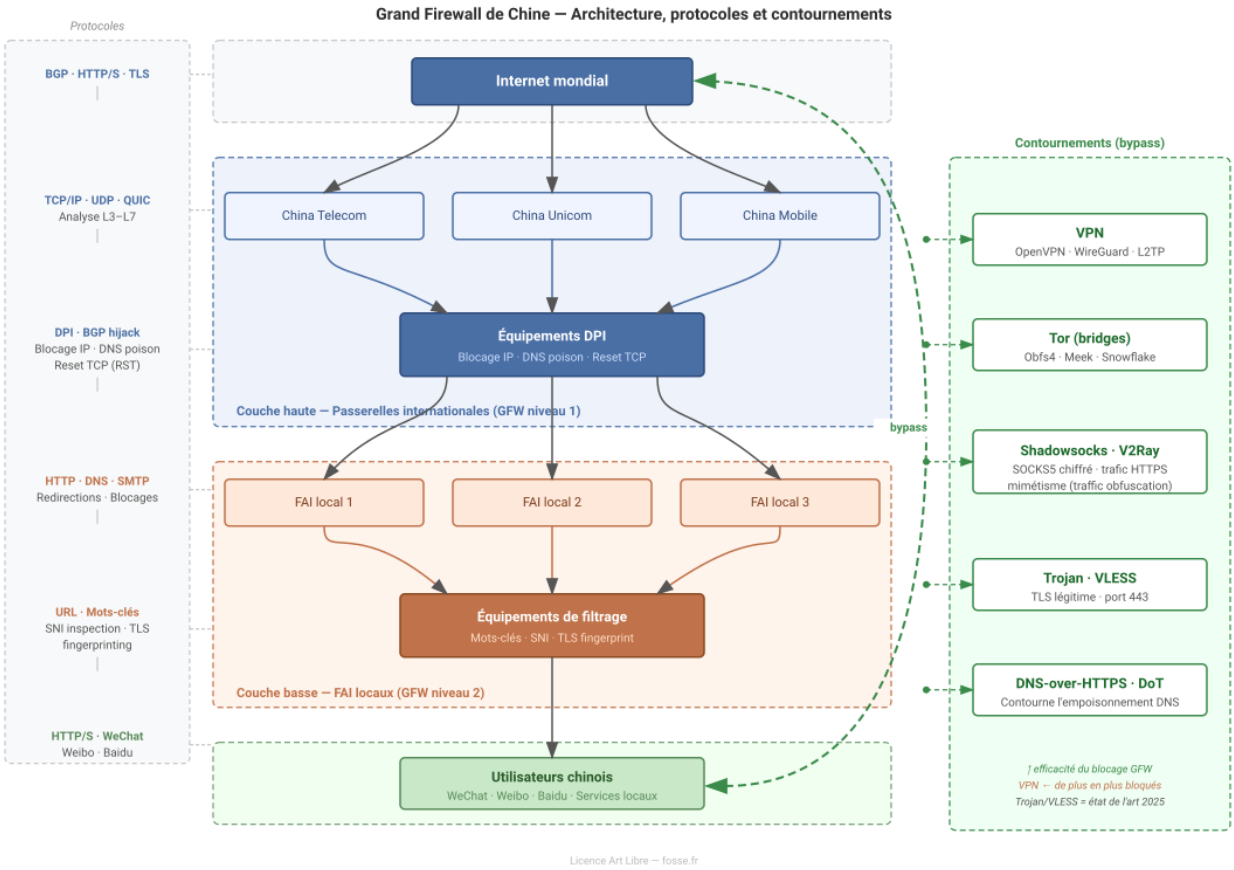

FIGURE 1 – Architecture, protocoles et contournements

et laissent des traces caractéristiques lors du traitement des connexions chiffrées [3]. Cette détection par empreinte de protocole a été progressivement étendue à Tor, à Shadowsocks et à d'autres outils de contournement.

En mai 2019, la Chine a déployé un système combinant analyse passive du trafic et sondage actif pour identifier les serveurs Shadowsocks : le GFW détecte d'abord les connexions suspectes par leur longueur et leur entropie, puis envoie des sondes actives au serveur cible pour confirmer sa nature. En réponse, les développeurs de Shadowsocks, V2Ray et Outline ont intégré des mécanismes résistants à ces sondes, les rendant à nouveau opérationnels en Chine jusqu'en septembre 2020.

Le 6 novembre 2021, de nouveaux blocages ont surpris les utilisateurs de Shadowsocks et VMess dans tout le pays. Ce blocage coïncidait avec la sixième session plénière du 19^{e} comité central du Parti communiste chinois (8-11 novembre 2021). Une équipe de chercheurs de l'Université du Maryland, de l'Université du Colorado Boulder, de l'Université du Massachusetts Amherst et du GFW Report a analysé ce nouveau mécanisme et publié ses résultats à la conférence USENIX Security 2023. Leur conclusion : le Grand Firewall applique désormais au moins cinq ensembles d'heuristiques pour identifier le trafic entièrement chiffré sans recourir au sondage actif — c'est la première fois qu'une telle détection purement passive est documentée à cette échelle [11].

La logique de détection est contre-intuitive : au lieu de définir ce qu'est le trafic chiffré, le système identifie ce qu'il n'est *pas*. Il exempte le trafic qui ressemble clairement à des protocoles connus (TLS, HTTP, SSH), puis bloque le reste. Ces heuristiques s'appuient sur les empreintes de protocoles connus, une mesure d'entropie (fraction de bits activés), et la proportion, la position ainsi que le nombre maximal continu de caractères ASCII imprimables dans le premier paquet TCP. Les chercheurs estiment que, si appliqué sans discrimination, ce mécanisme bloquerait environ 0,6 % du trafic internet normal en dommage collatéral. Le GFW limite donc son inspection à 26 % des connexions, ciblant spécifiquement les plages d'adresses IP des centres de données populaires utilisés par les services proxy.

Côté utilisateurs, les outils de contournement populaires — VPN, Shadowsocks, VMess, Obfs4 — font l'objet d'une surveillance permanente. Geedge Networks, l'entreprise de Fang Binxing dont les données ont fuité en 2025, documente explicitement dans ses procédures internes la méthodologie d'étude des VPN : abonnement à de multiples services commerciaux, décompilation statique du code source, analyse dynamique du trafic réseau dans des conditions contrôlées. La société revendique avoir « résolu » neuf grands fournisseurs VPN commerciaux [4].

Qu'est-ce que le système IJOP et comment surveille-t-il la population du Xinjiang ?

Le Grand Firewall censure ce que les citoyens peuvent lire. L'IJOP surveille ce qu'ils font. Ces deux systèmes coexistent dans un même État, mais l'IJOP représente une étape supplémentaire dans l'intrusion dans la vie privée : il ne filtre pas l'information, il modélise les individus.

La Plateforme opérationnelle conjointe intégrée (*Integrated Joint Operations Platform*, IJOP) a été déployée à partir de fin 2016 dans la région autonome ouïghoure du Xinjiang, dans le cadre de la « Campagne de répression sévère contre le terrorisme violent ». Le système est développé par Xinjiang Lianhai Cangzhi, filiale à 100 % de China Electronics Technology Group Corporation (CETC), un grand sous-traitant militaire d'État. En mars 2016, CETC avait annoncé publiquement avoir obtenu un contrat gouvernemental pour construire un programme de mégadonnées qui recueillerait des informations sur le comportement quotidien des citoyens et signalerait les activités inhabituelles pour anticiper le terrorisme.

Human Rights Watch a obtenu une copie de l'application mobile IJOP début 2018 et en a confié la rétro-ingénierie à la société berlinoise Cure53 fin 2018. L'analyse porte sur la version v2.1.2.7762, publiée le 20 novembre 2017. Les résultats sont publiés en mai 2019 dans un rapport de 68 pages [8].

L'application remplit trois fonctions : la collecte de données personnelles massives, le signalement d'activités ou de circonstances jugées suspectes, et le déclenchement d'enquêtes sur les personnes que le système désigne. Les données collectées vont de la couleur du véhicule à la taille précise au centimètre près, le tout relié au numéro de carte d'identité nationale. Le système suit les trajectoires de déplacement en surveillant en temps réel la localisation des téléphones, des cartes d'identité et des véhicules. Il surveille la consommation d'électricité et d'essence de la totalité de la population régionale. Les documents gouvernementaux du Xinjiang précisent que les données doivent être collectées « de manière exhaustive » auprès de « chaque personne dans chaque foyer ».

Quand l'IJOP détecte des irrégularités — un téléphone utilisé par une personne autre que celle à qui il est enregistré, une consommation d'électricité supérieure à la « normale », un déplacement hors de la zone de résidence sans autorisation policière — il signale ces « micro-indices » aux autorités comme autant de comportements suspects. Ces alertes constituent des motifs d'enquête, voire de détention.

La liste des comportements considérés comme suspects par l'application révèle l'étendue réelle du dispositif. L'utilisation de 51 outils réseau est signalée comme suspecte, dont WhatsApp, Viber et la plupart des VPN. Les activités religieuses licites sont surveillées : les dons aux mosquées, la prédication du Coran sans autorisation, les pèlerinages officieux à La Mecque. Des comportements tout à fait banals entrent dans les critères : ne pas

socialiser avec ses voisins, utiliser régulièrement une entrée secondaire plutôt que la porte principale, avoir des contacts avec l'étranger ou être apparenté à quelqu'un qui a récemment changé de numéro de téléphone. La possession d'appareils de sport comme du matériel de musculation est aussi documentée.

Le gouvernement chinois a par ailleurs procédé à la collecte d'échantillons d'ADN, d'empreintes digitales, de scans d'iris et de groupes sanguins de tous les résidents de la région entre 12 et 65 ans. Les prélèvements vocaux sont exigés lors des demandes de passeport. Thermo Fisher Scientific, entreprise américaine spécialisée en équipements de séquençage génétique, a fourni des analyseurs aux autorités du Xinjiang lors de la construction de cette infrastructure. Un généticien de l'Université Yale a collaboré en 2014 avec un chercheur du ministère de la Sécurité publique chinois en partageant des échantillons d'ADN permettant d'identifier l'appartenance ethnique ouïghoure à partir de matériel génétique.

Le résultat opérationnel de l'IJOP, c'est un système de « clôtures virtuelles » — l'expression est des autorités elles-mêmes, qui parlent de « filtres » et de « tamis ». Selon le niveau de menace calculé pour un individu, sa liberté de mouvement est restreinte à des degrés variables : certains sont détenus dans des camps d'« éducation politique », d'autres placés en résidence surveillée ou empêchés de quitter leur localité, d'autres encore interdits de voyager hors de Chine. Les estimations crédibles évoquent jusqu'à un million de personnes détenues dans ces camps. Les documents officiels du Xinjiang affichent sans détour l'objectif : « ceux qui doivent être arrêtés doivent être arrêtés », suggérant que maximiser le nombre de détentions est un indicateur de performance du système.

À quoi sert le Système de crédit social chinois et comment affecte-t-il les citoyens ?

Le Système de crédit social (SCS) est souvent présenté dans les médias occidentaux comme la pièce manquante d'un État-surveillance total : un score unique, calculé en continu, qui gouvernerait tous les aspects de la vie quotidienne. La réalité est plus fragmentée — et peut-être plus inquiétante par cette fragmentation même.

Le programme pilote a été lancé en 2014. Son objectif officiel est d'évaluer la « fiabilité » des citoyens, des entreprises et des organisations. Les données mobilisées couvrent les transactions financières, les comportements sur les réseaux sociaux, les activités en ligne, les dossiers gouvernementaux et les plateformes commerciales comme Alibaba et Tencent. Les mécanismes de sanction documentés incluent les interdictions de vol et de train, les restrictions d'accès aux établissements scolaires, la mise en liste noire pour des postes de la fonction publique et les expositions publiques d'individus jugés « non fiables ».

Des chercheurs de l'Université Duke et du *Journal of Politics* ont conduit une expérience de terrain auprès de 750 étudiants dans trois régions chinoises : révéler le potentiel répressif du SCS réduit significativement le soutien à celui-ci, tandis qu'insister sur sa fonction d'ordre social ne l'augmente pas [12]. L'explication tient dans une asymétrie d'information délibérément entretenue : la propagande d'État met en avant les avantages sociaux du système (lutte contre la fraude, respect des contrats), tandis que la censure supprime les informations sur ses usages répressifs. Les citoyens soutiennent ce qu'ils connaissent du système ; ils rejettent ce qu'ils en apprennent.

Ce que révèlent les études académiques, c'est que le SCS n'est pas un système unique et centralisé, mais une constellation de systèmes locaux aux règles hétérogènes. C'est précisément cette décentralisation qui le rend difficile à appréhender et à contester. La dimension politique est documentée : des gouvernements locaux ont utilisé ces systèmes pour réprimer des journalistes et bloquer des militants.

Qu'a révélé la fuite de données de Geedge Networks en septembre 2025 ?

Le 9 septembre 2025, une source anonyme a remis plus de 600 Go de données internes à la plateforme Enlace Hacktivista. L'origine : Geedge Networks et le laboratoire MESA (Machine Engineering and Systems Architecture Lab), deuxième division de recherche de l'Institut d'ingénierie de l'information de l'Académie des sciences de Chine. Les données couvrent Jira, Confluence, GitLab et des outils de gestion de projets internes. Une coalition de médias — le *Globe and Mail* canadien, le *Der Standard* autrichien, *Follow the Money*, *Paper Trail Media* — et d'organisations comme Amnesty International, le Tor Project, Justice For Myanmar et le laboratoire InterSecLab ont analysé les 100 000 documents pendant plusieurs mois avant la publication [2, 4, 7].

Geedge Networks a été fondée en 2018 par Fang Binxing, père du Grand Firewall, comme scientifique en chef. Le directeur technique est Zheng Chao, co-fondateur du laboratoire MESA. L'entreprise se présente comme un « fournisseur mondial d'équipements et de solutions de sécurité réseau et d'intelligence ». En pratique, les documents révèlent qu'elle commercialise une version exportable du Grand Firewall.

Le Kazakhstan est le premier client étranger de Geedge, dès 2019, après l'élection du président Kassym-Jomart Tokayev, dont la carrière diplomatique a débuté à l'ambassade soviétique à Pékin. Les images fuités exposent des

listes d'adresses IP d'un centre national et de 17 villes, utilisant trois produits Geedge distincts. L'Éthiopie suit vers 2021, en pleine guerre du Tigré : le système est utilisé pour détecter et maîtriser les troubles sociaux. Le Pakistan entre dans le dispositif en 2023, après que le canadien Sandvine a mis fin à son contrat sous pression des sanctions américaines ; Geedge reprend et améliore l'infrastructure existante pour mettre en place deux systèmes complémentaires, le *Web Monitoring System* (WMS 2.0) et le *Lawful Intercept Management System* (LIMS). Le Myanmar bascule en 2023, deux ans après le coup d'État militaire de février 2021 : Geedge aide la junte à bloquer 55 applications, dont les VPN, Tor, Signal et WhatsApp, en s'appuyant sur 13 opérateurs de télécommunications, des passerelles internet et 26 centres de données.

La suite logicielle de Geedge est architecturée autour de quatre composants principaux. Le *Tiangou Secure Gateway* (TSG) est le produit phare : un pare-feu de niveau national intégrant inspection profonde de paquets, détection et blocage des VPN, surveillance en temps réel des utilisateurs individuels et capacité d'injection de malware dans le trafic HTTP. Le TSG est conçu pour être interopérable avec un large spectre de matériels tiers afin de résister aux sanctions ciblées. Le *TSG Galaxy* est une infrastructure d'entrepôt de données qui agrège et stocke les données de l'ensemble du trafic internet des clients gouvernementaux. Le *Cyber Narrator* est l'interface utilisateur non-technique : les agents gouvernementaux peuvent interroger les données de surveillance, générer des graphes de relations à partir des contacts et des groupes en ligne d'un individu, et surveiller les comportements et les modes de vie. Le *Sanity Directory* (SAN) assure l'attribution réseau : en s'intégrant aux systèmes d'authentification des FAI (RADIUS, 3GPP, CGNAT), il lie le trafic réseau à des identités réelles via les données d'enregistrement des cartes SIM, elles-mêmes associées aux informations biométriques dans des pays comme le Pakistan.

Les capacités offensives documentées vont plus loin que la surveillance passive. Le DLL Active Defence fonctionne comme une plateforme DDoS-à-la-demande, comparable à celles disponibles sur le darkweb : il peut détourner les ordinateurs des utilisateurs pour les intégrer dans des botnets. Le système peut modifier en temps réel les sessions HTTP pour injecter du code malveillant dans des fichiers APK Android, des exécutables Windows, des images disque macOS, des paquets RPM Linux et des documents bureautiques. Il peut aussi injecter du JavaScript, du HTML et du CSS, et mener des attaques de type homme du milieu contre le trafic TLS.

La fuite révèle également que les données collectées sur les populations étrangères ne restent pas dans les pays clients. Les données TSG Galaxy sont accessibles aux employés de Geedge en Chine, et des instantanés sont parfois partagés avec des étudiants du laboratoire MESA pour des travaux de recherche. Cette exfiltration de données constitue une atteinte à la souveraineté des données des États clients — un angle mort que ces gouvernements ont délibérément ignoré.

Des composants de fabricants occidentaux apparaissent dans la chaîne d'approvisionnement. Sentinel HASP, un logiciel de protection de licence développé par une filiale du groupe Thales (France), est utilisé par Geedge pour gérer l'accès temporisé à ses logiciels. Le fabricant américain Niagara Networks a fourni des composants matériels pour le pare-feu pakistanais. Le FAI birman Frontiir, qui avait reçu des fonds d'investissement du Danemark, de Norvège et du Royaume-Uni, a installé dans ses centres de données les équipements Geedge permettant de tracer les utilisateurs et de bloquer les sites web et les VPN.

Geedge revendique desservir plus de 40 opérateurs mondiaux. Les offres d'emploi publiées mentionnent la Malaisie, Bahreïn, l'Algérie et l'Inde comme sites de déploiement. L'entreprise recrute également des traducteurs pour les marchés hispanophones et francophones. Le cadre de la Route de la Soie numérique (*Belt and Road Initiative*) constitue le vecteur principal de ce transfert technologique, reproduisant à l'international le modèle de contrôle politique développé au Xinjiang.

Conclusion

La fuite de 2025 n'est pas une révélation de plus dans une longue série. C'est la première fois qu'on dispose de la documentation interne complète d'un système conçu dès l'origine pour l'export. Ce qui était jusqu'ici observable depuis l'extérieur — des blocages, des ralentissements, des disparitions de contenus — devient lisible de l'intérieur : code source, fichiers de configuration, contrats, feuilles de route produit.

Ce qui se dessine dans ces documents, c'est moins une technologie qu'un modèle économique. Fang Binxing a construit le Grand Firewall pour l'État chinois. Il a ensuite fondé Geedge pour en commercialiser une version allégée, adaptable, interopérable, résistante aux sanctions. Le marché cible : les gouvernements qui souhaitent contrôler leur population en ligne sans avoir les ingénieurs pour le faire eux-mêmes.

La question qui reste ouverte n'est pas technique. Les contre-mesures existent — les chercheurs du GFW Report ont rapidement diffusé des stratégies de contournement après chaque mise à jour du système. La vraie question est politique : dans combien d'autres pays ces infrastructures sont-elles déjà opérationnelles, sous quelle identité juridique, et avec quels composants européens ou américains dans la chaîne d'approvisionnement ? La liste connue s'arrête à quatre pays. Le chiffre de 40 opérateurs mondiaux revendiqué par Geedge laisse une large marge à l'inconnu.

Références

[1] Birol Akduman. From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance. Anglais. In : *International Journal of Social Sciences* 7.28 (2023), p. 442-469.

[2] Sophia Baumann. China exports censorship tech to authoritarian regimes — aided by EU firms. Anglais. Follow the Money, sept. 2025.

[3] Sonali Chandel et al. The Golden Shield Project of China: A Decade Later — An in-depth study of the Great Firewall. Anglais. In : *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. IEEE, 2019, p. 111-119.

[4] Cybernews. Massive Great Firewall of China data leak reveals surveillance tech Silk Road. Anglais. Sept. 2025.

[5] Roya Ensafi et al. Analyzing the Great Firewall of China Over Space and Time. Anglais. In : *Proceedings on Privacy Enhancing Technologies* 2015.1 (2015), p. 61-76.

[6] GFW Report. Geedge Networks and MESA Lab Leak Analysis. Anglais. Sept. 2025.

[7] Global Voices Advox. How a Chinese company exports the Great Firewall to autocratic regimes. Anglais. Sept. 2025.

[8] Human Rights Watch. China's Algorithms of Repression — Reverse Engineering a Xinjiang Police Mass Surveillance App. Anglais. Human Rights Watch, mai 2019.

[9] Jyh-An Lee. Great Firewall. Anglais. Research Paper 2018-10. The Chinese University of Hong Kong, Faculty of Law, 2018.

[10] Yao Wang et Andrew Dobson. We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies. Anglais. In : *Global Media and China* 4.2 (2019), p. 220-232.

[11] Mingshi Wu et al. How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. Anglais. In : *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, 2023.

[12] Xu Xu. To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. Anglais. In : *American Journal of Political Science* (2021).